Gratis magasin om sikkerhed på nettet • oktober 2008

netsikker nu!
magasinet



GØR DIN PC TOPSIKKER
Så let holder du hackere og virus på afstand – gratis!

Surf trygt på nettet

DE BEDSTE TIPS & TRICKS
- Gør Internet Explorer bomstærk
- Få dig et robust kodeord
- Hold pc'en opdateret

Test dig selv: Er du sikker på nettet?



SÅDAN AFSLØRER DU SVINDLERNE

10 GODE RÅD, NÅR UNGERNE GÅR ONLINE

Vær klar til en overraskelse:

SÅ MEGET VED NETTET OM DIG

\+ Vind supersikre USB-nøgler + Stor guide til de bedste programmer + Sådan beskytter du dig let på nettet + Få en digital signatur

Gratis



Sådan surfer du trygt på nettet

Internettet bugner af gode oplevelser og masser af indhold, men er desværre også et eldorado for svindlere. Med din kritiske sans – og måske lidt inspiration fra dette magasin – kan du dog ganske roligt bevæge dig ud på nettet.

Tip 1 Brug din kritiske sans

Støder du på noget, der virker for godt til at være sandt – så er det nok ikke sandt. Løfter om gratis ting eller hurtige gevinster er eksempler på e-mails, du som regel bare kan slette med det samme. Det gælder især, hvis de kommer fra ukendte personer eller indeholder vedhæftede filer.

Læs mere i historien "Undgå at falde for svindlernes mails" på side 14

Tip 2 Er du i tvivl? Så slet eller luk

Stol altid på din intuition. Hvis du fornemmer, at noget ikke er, som det burde være, så slet straks den mistænkelige mail fra din indbakke – eller luk din browser, hvis det er en hjemmeside, der bekymrer dig. Tastekombinationen Alt + F4 er den mest effektive måde at lukke en side hurtigt på.

Se, hvordan du gør Internet Explorer topsikker, på side 24

Tip 3 Hold din pc opdateret

Når hackere og virus slår til, skyldes det ofte, at de har udnyttet fejl i et program eller i Windows til at få kontrol over din pc. Sørg altid for at have opdateret dine programmer og især dine sikkerhedsprogrammer – antivirus, firewall og antispyware – og sæt også Windows til selv at hente nye opdateringer.

Stor guide på side 4: Gratis programmer gør din pc til et fort

Tip 4 Brug stærke – og mange – kodeord

Det tager en erfaren hacker 12 sekunder at knække et almindeligt kodeord på fem små bogstaver – og hvis du bruger det samme kodeord mange steder, har han pludselig fri adgang til alle dine personlige oplysninger. Hav som minimum seks tegn, et eller flere store bogstaver samt tal i dit kodeord, og brug forskellige kodeord på forskellige sider.

Se på side 23, hvordan du gør dit kodeord superstærkt

Tip 5 Vær på vagt, når det handler om penge

Du skal som udgangspunkt aldrig udlevere dankortoplysninger, CPR-nummer, pinkoder, adgangskoder osv. i e-mail eller på nettet. Dog er det selvfølgelig i orden at indtaste dankortoplysninger, hvis du handler i en netbutik, du har tillid til, og også at indtaste dit CPR-nummer, hvis du er inde på en sikker side hos en offentlig myndighed.

Læs om sikker netbank på side 18 og om digital signatur på side 26

netsikker nu!-magasinet

Produceret af



til kampagnen netsikker nu!
www.netsikkernu.dk

Redaktør: Rasmus Udsholt

Skribenter: Chris Hansen, Thomas O. Nielsen, Henning Rasmussen, Steffen Slumstrup Nielsen, Torben B. Sørensen og John Alex Hvidlykke

Layout: Martin Andersen/18k og Elisabeth S. von Eyben

Fotos: Stillleben og iStockphoto©

Chefredaktør: Leif Jonasson

Tryk: Color Print A/S

Kontakt til redaktionen:
red@komputer.dk

Helt sikker på nettet



Danmark er et af verdens førende lande, hvad angår befolkningens brug af internettet. Flere og flere har taget nettet til sig som en naturlig del af deres hverdag. I langt de fleste tilfælde får vi gode oplevelser ved at færdes på internettet.

Desværre sker det også fra tid til anden, at vi i vores færden på nettet oplever situationer, som vi ikke havde forudset. Det skyldes ofte, at andre mennesker forsøger at udnytte vores brug af internettet. For at undgå dette er det vigtigt, at vi er opmærksomme på sikker adfærd på nettet, og at vi inddrager it-sikkerhed som en del af vores hverdag.

For at skabe gode vilkår for befolkningens brug af internettet afvikler Videnskabsministeriet i samarbejde med en lang række danske virksomheder kampagnen "netsikker nu!". Dette magasin er et led i denne kampagne.

netsikker nu! arbejder for, at danskerne skal blive mere fortrolige med it-sikkerhed og øge sikkerheden på egne medier. Kampagnen sætter fokus på aktuelle it-sikkerhedsproblemer, som vi kan støde på i vores færden på internettet, og hvordan vi kan undgå eller afhjælpe dem.

I 2008 retter netsikker nu! et særligt fokus på områderne:
• Privatlivets fred på internettet
• Misbrug og mistillid på internettet
• Opdatering af din computer

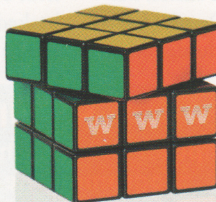
Temaerne er valgt på baggrund af den voksende udbredelse af sociale netværkstjenester og befolkningens stigende interesse for at offentliggøre personlige data på internettet.

I dette magasin giver netsikker nu! dig en række gode råd om, hvordan du kan blive mere sikker, når du færdes på internettet.

God fornøjelse.

Helge Sander, videnskabsminister

Indhold





Gratis programmer gør din pc til et fort

En Windows-maskine er forholdsvis sikker, men du er nødt til også selv at yde en indsats, hvis du vil undgå både virus, hackere, spam og svindlere. Her viser vi dig fem effektive trin til at gøre pc'en til en fæstning. **Af Henning Rasmussen**

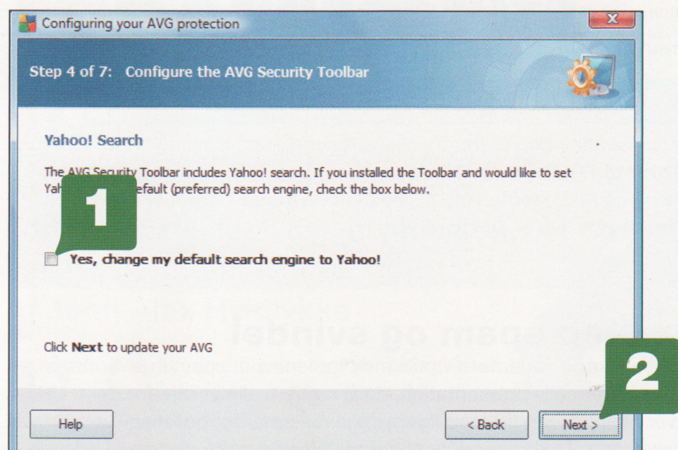
Selv om de nyeste udgaver af Microsofts udbredte styresystem Windows er sikrere end nogen sinde før, kan du ikke overlade hele din sikkerhedsstrategi til hverken Vista eller XP alene. Begge udgaver af Windows har godt nok en simpel firewall til at holde hackere ude, men du er bedre sikret, når du installerer en "rigtig" firewall. Og når det handler om virusbeskyttelse, så er du slet ikke beskyttet i Windows XP og kun i begrænset omfang i Windows Vista. Her er det altså helt afgørende, at du hurtigst muligt får installeret et program, der kan få bugt med de ondsindede filer. Det samme gælder den type svindel, der kaldes phishing – en form for kriminalitet, hvor svindlere sender dig mails, der fx ligner beskeder fra din bank. Formålet er at lokke dig ind på falske hjemmesider og få dig til at indtaste dine personlige oplysninger og log-in til din netbank, så bagmændene kan lænse din konto for kontanter. Det kan du alt sammen undgå ved at følge guiden på de næste sider her i magasinet. Vi fortæller om de bedste gratis sikkerhedsprogrammer, ligesom vi viser, hvordan du kommer i gang med programmerne. Du finder alle de omtalte programmer på **www.komputer.dk/netsikker**

Få alle programmerne gratis

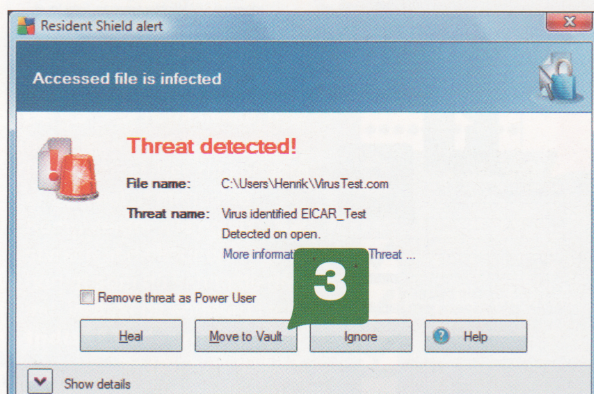
På magasinet Komputer for alles hjemmeside finder du alle de links, du skal bruge til at hente programmerne kvit og frit: www.komputer.dk/netsikker

1 Beskyt pc'en mod virus

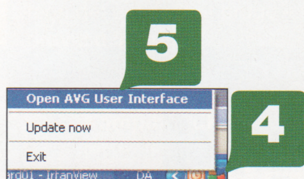
I Windows XP findes der ingen indbygget beskyttelse mod virus, mens Vista kan fange enkelte typer. Du kan altså ikke klare dig uden et godt antivirusprogram – som dog heldigvis ikke behøver koste noget som helst. Du kan fx installere det gratis antivirusprogram AVG Free 8.0 og herunder kan du se, hvordan du installerer og bruger programmet.



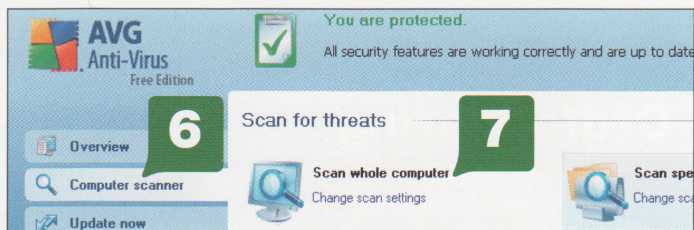
1 Dobbeltklik på filen, når den er hentet fra nettet. Under installationen foreslår AVG Anti-Virus, at du ændrer din standard-søgemaskine til Yahoo!. Hvis du er tilfreds med din nuværende søgemaskine, fx Google, bør du sige nej ved at fjerne fluebenet i feltet **(1)**. Klik derefter på **Next (2)**, og genstart pc'en, når du bliver bedt om det. Når du tænder computeren igen, er den sikret mod virus.



2 Hvis AVG Anti-Virus finder en virus, får du straks besked. Vil du være på den sikre side, bør du klikke på **Move to Vault (3)**, der flytter virussen væk til nærmere analyse. AVG Anti-Virus vil i nogle situationer foreslå **Remove threats** i stedet, og det er også fint.



3 Så snart AVG Anti-Virus er installeret, bør du scanne din pc's drev for virus. Programmet scanner både cd'er, dvd'er, USB-nøgler og harddiske. Højreklik på AVG's firefarvede ikon i systembakken **(4)** nederst til højre i Windows, og vælg **Open AVG User Interface (5)**.

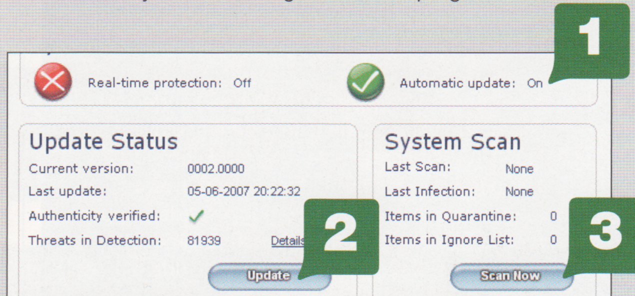


4 Nu åbner hovedvinduet i AVG Anti-Virus. Klik på **Computer scanner (6)** og derefter på **Scan whole computer (7)**. Efter et stykke tid får du resultatet, som gerne skulle vise nul virus. Hvis der skulle være virus, bliver det automatisk fjernet af AVG Anti-Virus. Klik på **Close results** for at lukke vinduet. AVG fortsætter med at køre i baggrunden.

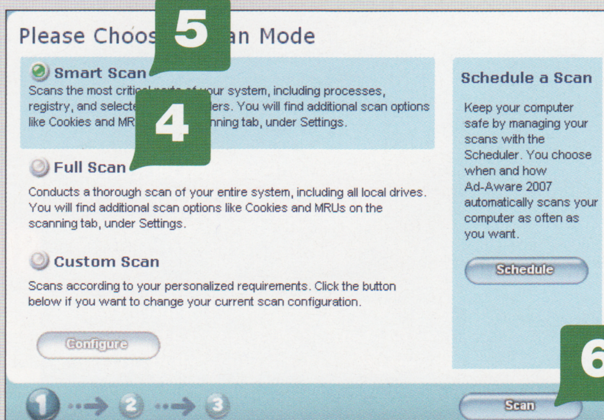
TIP AVG opdaterer sig selv, hvis din internetforbindelse altid er tændt – og ellers kan du manuelt opdatere programmet, så det kender de nyeste virus, ved at højreklikke på AVG's firefarvede ikon i systembakken nederst til højre i Windows og vælge **Update now**.

2 Undgå reklamer og spioner på computeren

Når du fx installerer gratis programmer fra nettet, risikerer du indimellem, at der følger såkaldte reklame- eller spionprogrammer med. Reklameprogrammerne holder øje med din færden på nettet, så reklamer kan målrettes til dig, mens spionprogrammerne kan være langt farligere, da formålet kan være at opsnappe personlige oplysninger fra dig. Hvis du allerede har antivirusprogrammet AVG Anti-Virus Free 8.0 installeret, er du beskyttet mod disse spionprogrammer, men for en sikkerheds skyld kan du fx også installere programmet Ad-Aware.



1 Hent Ad-Aware og installer det. Når du starter det første gang, fortæller programmet, at automatisk opdatering er aktiveret **(1)**. Klik på **Update (2)** for at hente den nyeste opdatering med det samme. Klik så på **Scan Now (3)** for at scanne din pc.



2 Første gang du bruger programmet, bør du klikke på **Full Scan (4)** for at scanne hele pc'en. Næste gang kan du nøjes med den mindre omfattende **Smart Scan (5)**. Klik på **Scan (6)** i bunden for at starte.



Ordforklaring

Antivirus: Et antivirusprogram er et program, som ligger i baggrunden og holder øje med de andre programmer, der kører på din pc. Hver gang du fx åbner et program eller læser en mail, tjekker antivirusprogrammet, om programmet eller mailen indeholder nogen af de virus, som det kender. Når du installerer et antivirusprogram, vil det normalt som det første tjekke hele din harddisk for virus.

Firewall: En firewall er et program eller en særlig computer, der bruges til at sikre computerne på indersiden af firewallen mod angreb (fx fra hackere) fra den ydre verden. Firewallen bruger såkaldte portnumre til at afgøre, om en pakke med data skal have adgang til din computer – og som regel tillader en firewall kun indkomne pakker, der er svar på henvendelser, som pc'en selv har afsendt.

Hacker: Person, som uden tilladelse bryder ind på en anden computer. Hackere kan lave indbruddet for at skaffe sig adgang til informationer, stjæle programmer eller simpelt hen som en intellektuel udfordring.

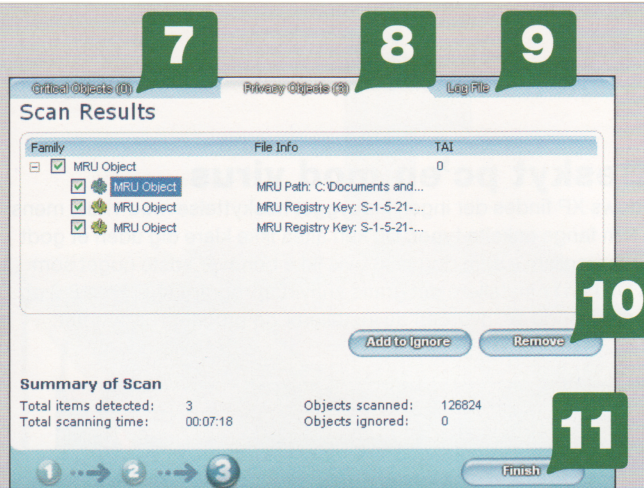
Orm: En orm er en slags computervirus, som er kendetegnet ved, at den formerer sig kraftigt – som regel via internettet eller et andet netværk. Ormen udnytter svagheder i programmer, og når den først er kommet indenfor på pc'en, bruger den computeren som base for nye angreb ved at søge efter andre maskiner på netværket, der også er sårbare. Da en orm ikke kræver medvirken fra mennesker, kan den på kort tid sprede sig og ramme en meget stor mængde computere.

Spam: Typisk reklame-mails af den ene eller den anden art, som sendes uopfordret til din postkasse. Spam er ulovligt i mange lande, men spammerne er svære at fange og sidder ofte i et andet land end modtageren. Pas på med, hvem du giver din e-mail-adresse til. Hvis du deltager i nyhedsgrupper, postlister og tvivlsomme konkurrencer på spilhjemmesider, hvor du afgiver din e-mail-adresse, er du ofte selv ude om, at du modtager spam-mails.

Spyware: Små "reklamefinansierede" spionprogrammer, der i al hemmelighed kan blive installeret på din computer, fx når du downloader ting fra internettet. Et spyware-program indsamler oplysninger, som det sender tilbage til programmøren eller det firma, der leverer reklamerne. Spyware kan fjernes med et antispywareprogram som fx Ad-Aware.

Sårbarhed: En fejl i et program, der udgør et sikkerhedsproblem. Det kan fx være en fejl, der giver uvedkommende mulighed for at køre et program på pc'en. Stort set alle programmer har sårbarheder – men mange af dem er ikke opdaget. For at sikre dig skal du aktivere de automatiske opdateringer i Windows og holde dine programmer opdateret – så bliver de opdagede sårbarheder rettet hurtigst muligt.

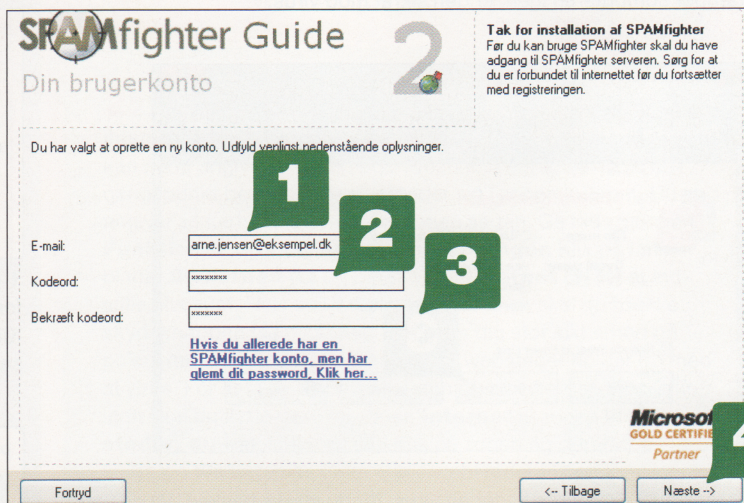
Trojansk hest: Et program, som smugler en virus ind i din pc ved at foregive at være et andet program. Trojanske heste er "snydeprogrammer", som under dække af et harmløst udseende program, fx et spil, smugler skadelige programmer ind i din computer. Det skadelige program kan være en virus eller et fjernstyringsprogram, der kan bruges af hackere til at tage kontrol over din pc. Trojanske heste vil blive opdaget af et godt og opdateret antivirusprogram.



3 Når scanningen er færdig, vises resultatet på tre faneblade: **Critical Objects (7)**, **Privacy Objects (8)** og **Log File (9)**. Du fjerner spionerne og reklamerne ved at klikke på **Remove (10)**. Klik til sidst på **Finish (11)**. Nu er din pc renset.

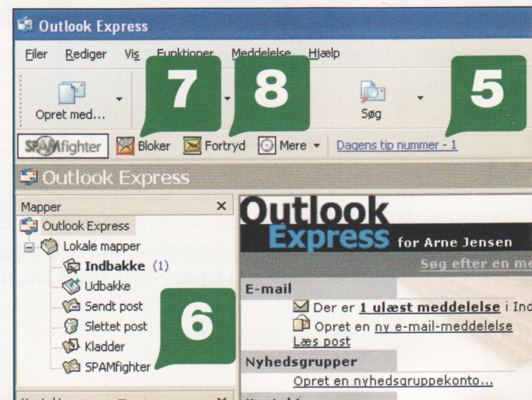
3 Stop spam og svindel

De uønskede reklame-e-mails med kælenavnet spam kræver næppe nogen nærmere præsentation, da vi næsten alle er ofre for dem. Ud over at spilde din tid med ligegyldige reklamer for potenspiller og piratsoftware, så rummer nogle af meddelelserne også direkte svindelforsøg, hvor bagmænd fx forsøger at lokke dig til at sende personlige oplysninger til dem. Hvis du bare sletter disse meddelelser, sker der dog intet. Med programmet SPAMfighter slipper du endda stort set selv for at sortere spam-meddelelserne fra i dit e-mail-program.



1 Hent og installer SPAMfighter. Luk dit e-mail-program – fx Outlook Express i Windows XP eller Windows Mail i Vista. Start SPAMfighter. Først skal du oprette en brugerkonto. Udfyld din mailadresse **(1)**, og vælg et kodeord **(2)**. Indtast kodeordet igen **(3)**, og klik på **Næste (4)** et par gange for at afslutte guiden.

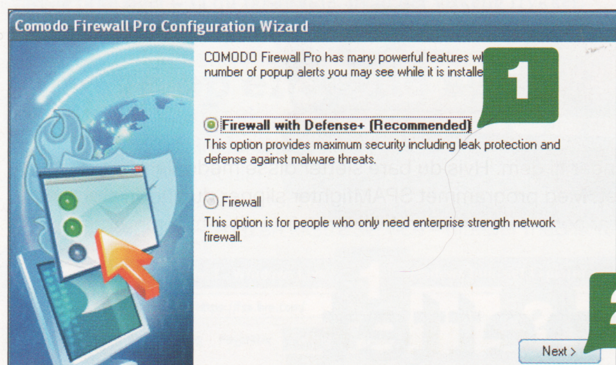
2 Åbn dit e-mail-program. SPAMfighter har nu installeret en værktøjslinje i programmet **(5)**. Fremover vil programmet automatisk holde øje med spam-mails og flytte dem til



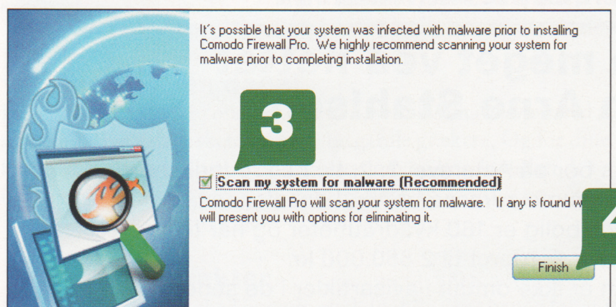
mappen **SPAMfighter (6)**. Du bør tjekke mappen indimellem for at være sikker på, at programmet ikke ved en fejl har lagt en mail fra en af dine venner i mappen. Hvis du modtager en spam-mail, som SPAMfighter ikke opdager, kan du klikke på mailen og derefter på **Bloker (7)** for selv at stemple mailen som spam. Mailen flyttes samtidig til mappen **SPAMfighter**. Med **Fortryd (8)** kan du fortryde, at du har markeret en mail som spam. Det fjerner mailen fra mappen **SPAMfighter** igen.

4 Hold hackerne ude

Internettet benyttes ikke kun af lovlydige og fredsommelige folk. Der findes – præcis som i det rigtige samfund – desværre også mennesker med onde hensigter. I denne kategori er hackeren, der ved hjælp af værktøjer forsøger at plante skadelig kode på din maskine, så den kan fjernstyres til kriminelle formål – fx at lægge en hjemmeside ned ved at bombardere den med millioner af besøgende på én gang. Med en god firewall nægter du hackeren adgang til din pc. Prøv fx den gratis firewall Comodo Firewall Pro. Her viser vi, hvordan du kommer i gang med den.



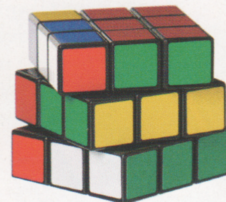
1 Dobbeltklik på filen, når den er hentet fra nettet. Du må ikke have andre firewalls installeret – det skal du bekræfte, at du ikke har, ved at klikke på **Ja** på første skærmbillede. Klik på **Next** i det næste vindue og så på **I ACCEPT**, når du bliver spurgt, om du accepterer licensbetingelserne. Sæt markering i **Firewall with Defense+ (Recommended) (1)** – så installerer du både firewall og funktionen Defence+, som beskytter din pc, hvis der alligevel er sluppet skadelige programmer ind på den. Klik på **Next (2)** og på **Next** igen i det næste programvindue.



2 For at sikre, at din pc ikke allerede er inficeret med virus eller spyware, skal installationsprogrammet scanne maskinen, så skadelige programmer kan blive fundet og fjernet. Sæt et flueben ud for **Scan my system for malware (3)**, og klik på knappen **Finish (4)**. Efter nogen tid vil du blive bedt om at genstarte pc'en. Herefter beskytter Comodo Firewall Pro din pc. Når pc'en er genstartet, popper en meddelelse fra Comodo Firewall op med overskriften **New Private Network Detected!**. Meddelelsen betyder, at firewallen har registreret, hvilket netværk din pc er tilsluttet. Du kan give netværket et navn – fx Hjemme – men det er ikke en nødvendighed. Klik på **OK**.

TIP

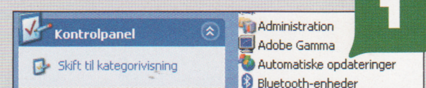
Comodo advarer, når programmer opfører sig mistænkeligt. Klik på **Allow this request**, hvis du kender og har tillid til programmet. Ellers bør du klikke på **Block this request**. Indtil firewallen kender din pc, vil du ofte opleve advarslerne – herefter vil du sjældent støde på dem, især hvis du ved hvert svar også vælger **Remember my answer** (husk mit svar). Når du installerer nye programmer eller fx opdaterer Windows, vil du ofte opleve, at du skal vælge **Allow this request** vældig mange gange, fordi programmet installerer forskellige dele rundt omkring på pc'en. Hvis du bliver træt af dette, så vælg **Treat this application as Installer or Updater**, og klik på **OK**. Så lader din pc programmet gennemføre installationen uden at gribe ind.



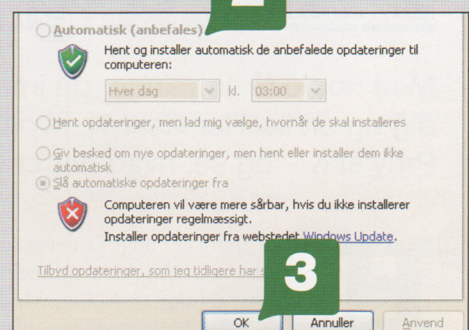
5 Husk at opdatere Windows

Der bliver jævnligt fundet nye huller i Windows' sikkerhed – heldigvis retter Microsoft dem løbende, når de opdager dem. Men det kræver selvfølgelig, at du holder dit Windows opdateret – gerne med automatiske opdateringer, så hullerne lukkes af sig selv. Her kan du se, hvordan du opdaterer henholdsvis Windows XP og Vista.

Sådan opdaterer du XP

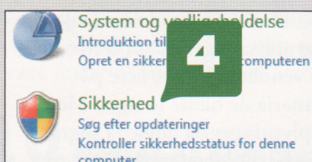


1 Klik på Startknappen i bunden til venstre, og vælg **Kontrolpanel**. Dobbeltklik på **Automatiske opdateringer (1)**.

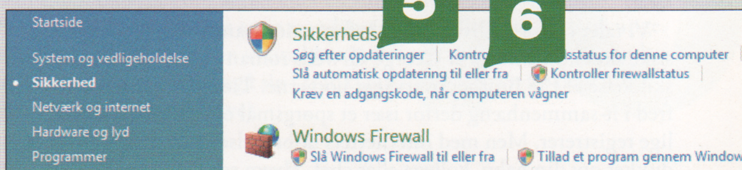


2 Sæt markering i **Automatisk (anbefales) (2)** – så henter og installerer Windows selv opdateringer, efterhånden som de bliver tilgængelige. Klik på **OK (3)**.

Sådan opdaterer du Vista



1 Klik på Startknappen i bunden til venstre, og vælg **Kontrolpanel**. Klik på **Sikkerhed (4)**.



2 Du kan søge efter opdateringer straks ved at klikke på **Søg efter opdateringer (5)**. Hvis automatiske opdateringer ikke er slået til på maskinen, kan du klikke på **Slå automatisk opdatering til eller fra (6)** for at slå funktionen til.



Find dig selv på nettet

Med nogle få søgninger på internettet kan helt fremmede mennesker finde mange oplysninger om dig og dit liv. Her viser vi, hvor nemt det er at finde informationer om en persons bolig, job og fritid. Prøv selv – og se, hvad nettet ved om dig. Af Torben B. Sørensen

Hvad ved andre om mig? Det er et spørgsmål, vi måske ikke lige stiller til daglig. Men indimellem bliver det aktuelt. Måske har du søgt en stilling. Måske har du mødt en ny kæreste. Eller måske er du bare blevet nysgerrig: Hvad kan andre finde ud af om dig – og hvad kan du selv finde ud af om andre? Og er der noget af det, som du ville foretrække, at de ikke kunne finde?

Nettet har en fantastisk hukommelse. Derfor skal man overveje det grundigt, før man lægger personlige oplysninger ud, så resten af verden kan se dem. Det er rart for dine venner at kunne læse på Facebook, at du nyder livet på Gran Canaria de næste to uger. Men en indbrudstyv kan ud fra de samme oplysninger og nogle få søgninger finde frem til din adresse og bryde ind i dit hjem, mens du er på ferie.

Vi taler om privatlivets fred i informationssamfundet, og det klassiske skræmmebillede er George Orwells roman "1984", hvor staten i skikkelse af Big Brother overvåger borgerne. Tidligere var privatlivets fred i it-sammenhæng derfor især et spørgsmål om, hvad det offentlige registrerer. Men med internettets udbredelse er en ny Big Brother dukket op: din nabo, kollega eller chef. Hvem som helst med en pc og adgang til internettet kan nu søge efter oplysninger om dig.

Hvad kan de finde? Det kan du let få svar på. Du skal blot udføre de samme søgninger, som andre kan foretage. Som eksempel har vi søgt efter information om en person. Af hensyn til hans privatliv har vi valgt at anonymisere søgningerne. Men de bygger alle på data, som vi har fundet via offentligt tilgængelige websider. Vi kalder vores hovedperson for Arne Stahlson. Du kan prøve at udføre de følgende søgninger med dig selv som emne:

Så meget ved nettet om Arne Stahlson

- Han bor på Astersvej 2, 2. tv. på Frederiksberg.
- På samme adresse bor en Lene Jensen.
- Hans bolig er 160 kvadratmeter og har fem værelser.
- Den er vurderet til 2.850.000 kr.
- Han er ikke omtalt i avisartikler i de senere år.
- Han sidder i direktionen for tre anpartsselskaber.
- Han har øjensynlig ikke skrevet bøger.
- Han har registreret tre domænenavne på internettet, der alle har tilknytning til de virksomheder, han er direktør for.
- Han gennemførte Jyske Bank-løbet 2006, 4 km, i tiden 00:23:38.
- På sin LinkedIn-profil oplyser han, at han er interesseret i at høre om ledige job.

Adresse og telefonnummer

Vores søgning starter på De Gule Sider. Hvis personen har telefon, findes han som regel her. En indtastning af "Arne Stahlson" giver en stribe kandidater med samme eller lignende navne. Hvis der er for mange, kan vi begrænse mængden, hvis vi også ved noget om, hvor han bor henne. En anden nem indgang er at indtaste et telefonnummer på personen. Resultatet fortæller navn, adresse og diverse andre telefonnumre.

Er Arne enlig, eller har han en kone eller kæreste? Ved at søge efter adressen uden at skrive hans navn finder vi ud af, om der er registreret andre personer på samme adresse. Her er der dog grund til at være kritisk: Data er ikke altid opdateret, så måske står der opført en person, som tidligere har boet på samme adresse. Desuden fremgår det ikke, om den anden person på adressen har lejet et værelse eller indgår i husstanden.

www.degulesider.dk: På De Gule Sider kan du finde en persons adresse og telefonnummer. Ved at søge på adressen alene kan du se, om der bor andre samme sted. Indtast dit eget navn i feltet **Hvem/hvad** **(1)**, og klik på **Søg** **(2)** – og hvis der findes flere med samme navn, kan du indsnævre søgningen ved også at indtaste et bynavn.

Hvad bor han i?

Når vi har adressen, kan vi også finde ud af noget om Arne Stahlsons boligforhold: Hvad er hans bolig værd? På SKATs webside finder vi den seneste ejendomsvurdering, der blev foretaget i 2007. Vi indtaster kommune, vejnavn og husnummer, og straks får vi en oversigt over vores hovedpersons boligforhold. Det kræver dog, at han bor i en ejerbolig, for leje- og andelslejligheder er ikke med.

www.vurdering.skat.dk/Ejendomsvurdering: På SKATs hjemmeside kan du finde alle offentlige ejendomsvurderinger. Fx af den ejendom, du bor i – hvis det er en ejerbolig. Indtast kommunenavnet **(3)** og adressen **(4)**, og klik derefter på **Søg** **(5)**.

Nu får du oplyst den offentlige grund- og ejendomsværdi **(6)**.

Grundværdi	Ejd.værdi:	
293.800	2.000.000	Vurdering
584.400	2.850.000	Vurdering

Men uanset boligtypen kan vi finde ud af mere om den. BBR (Bygnings- og Boligregistret) indeholder oplysninger om alle ejendomme i landet. Adgang til BBR sker via Den Offentlige Informationsserver, OIS.dk. Man skal blot indtaste adressen. En søgning her viser, at Arne bor på 160 kvadratmeter og har fem værelser. Og så er der en verserende byggesag.

www.ois.dk: På Den Offentlige Informationsserver har du adgang til at søge i Bygnings- og Boligregistret og finde oplysninger om alle ejendomme i landet. Indtast kommunenavnet **(7)** og adressen **(8)** i felterne øverst til højre, og klik på **Søg** **(9)**.

Nu kan du blandt andet se ejendommens størrelse **(10)**, antallet af værelser **(11)** og andre informationer om ejendommen.

Én ting er den offentlige vurdering. Men hvis Arne har købt sin bolig inden for de seneste år, kan vi også finde ud, hvad han reelt har givet for den. Nyere tinglyste skøder kan findes via Statstidende. Man indtaster blot adressen i søgefeltet på **www.statstidende.dk** for at se de skøder, der er tinglyst. I nogle tilfælde optræder prisen for ejendommen dog ikke. Statstidende lader dig også tjekke, om en person har optaget lån i sin bil eller bolig, og om han har været igennem en gældssanering.

www.statstidende.dk: Statstidende fortæller, hvem der har købt og solgt en ejendom, og hvad den kostede. Indtast adressen **(12)** i søgefeltet til højre på forsiden, og klik på **Søg** **(13)**. I stedet kan du også taste et navn i søgefeltet for at se, om personen for nylig har været omtalt i Statstidende – fx i forbindelse med gældssanering.

>>>

5 gode råd om privatliv på nettet

1. Læs altid vilkår og privatlivs-politikken på den netværkstjeneste, du befinder dig på. Hvis du ikke er opmærksom, kan netværks-tjenesten fx anvende dine personlige billeder i en reklame uden at spørge dig yderligere om lov.

2. Vær altid opmærksom på brugen af applikationer (små programmer) som fx quizzer på netværks-tjenesterne. Hvis du tilføjer applikationen til din profil, giver du også ejeren af applikationen adgang til dine personlige oplysninger.

3. Begræns altid adgangen til dine private oplysninger, såsom adresse, telefonnummer, e-mail og CPR-nummer. Husk fx altid at fjerne dit CPR-nummer, hvis du lægger dit CV på nettet.

4. Tænk generelt over, hvad du skriver og lægger på din profil. 20 procent af alle arbejdsgivere søger informationer om potentielle medarbejdere på nettet, og hvem ønsker, at den fremtidige chef får adgang til billeder af dig fra en fest for ti år siden? Tænk derfor også over, hvad du offentliggør om andre personer.

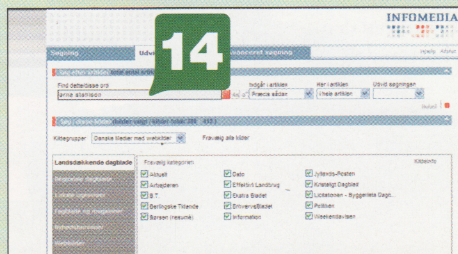
5. Vær altid kritisk, når du modtager invitationer og andre forespørgsler på nettets sociale netværk. Hvis du accepterer en invitation, giver du nemlig afsenderen adgang til din profil.



De fem gode råd kommer fra Sarah Kirkeby, der er privacy-ekspert i IT- og Telestyrelsen.

Har han været i avisen?

Hvis du søger efter en person, som pressen har skrevet om, kan du finde frem til artiklerne. Det kræver dog lidt ekstra arbejde. Artikler fra dagblade, Ritzaus Bureau og en række fagblade og tidsskrifter er samlet i databasen Infomedia. Men det koster penge at få adgang. De danske biblioteker har imidlertid et fælles abonnement på tjenesten. Hvis dit lokale bibliotek tilbyder trådløs adgang, kan du tage din egen pc med og søge i Infomedia fra den. Ellers kan du bruge en af bibliotekets pc'er. Vores søgning efter Arne Stahlson giver dog intet resultat. Han har åbenbart ikke været i mediernes søgelys.

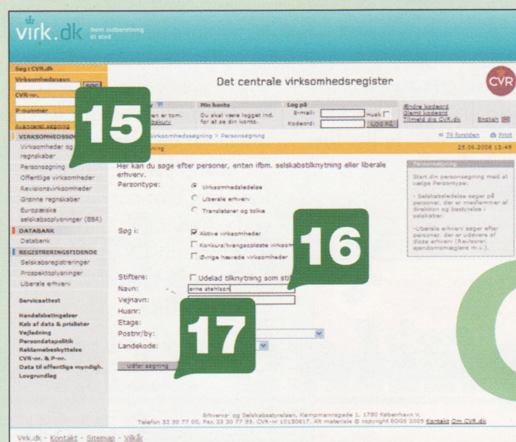


Avis omtale?

www.infomedia.dk: Gå på biblioteket og søg i dagbladenes database, Infomedia, efter avisomtale. Prøv at indtaste dit navn i feltet **Find dette/disse ord (14)**, og tryk på **Enter** på tastaturet.

Hvem er hans netværk?

Måske er vores hovedperson forretningsmand. Han kan sidde i bestyrelser eller være medejer af virksomheder. I så fald kan du finde ham i Det Centrale Virksomhedsregister (CVR). Under person-søgning kan du indtaste navn og andre oplysninger. Søgeresultatet fortæller, hvilke virksomheder personen er tilknyttet.



netværk? CVR

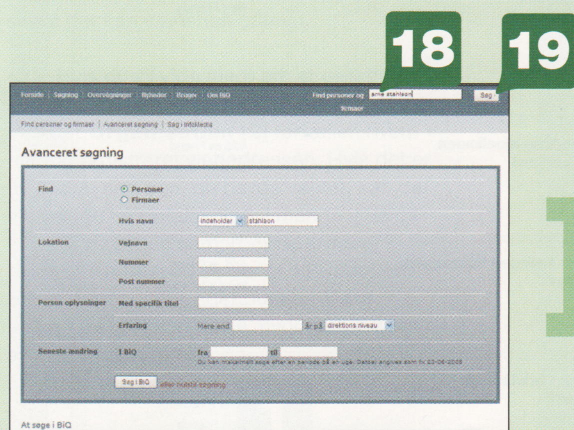
www.cvr.dk: En søgning i CVR-registret viser, hvilke firmaer en person er tilknyttet. Klik på **Personsøgning (15)**, tast derefter navnet i feltet **Navn (16)**, og klik på **Udfør søgning (17)**.



virk.dk

CVR-søgningen viser i dette tilfælde, at Arne Stahlson er tilknyttet tre virksomheder.

Hvis erhvervsvinklen viser sig interessant, kan du fortsætte ad det spor. Her er tjenesten BiQ nyttig. Den koster penge, men du kan prøve den gratis i en uge. BiQ samler informationer fra CVR, KOB (det tidligere Købmandsstandens Oplysning), Statstidende, andre databaser og virksomhederne selv. En af de smarte finesser ved BiQ er muligheden for at se en persons netværk: Man kan se, hvilke personer han sidder i bestyrelse med eller på anden måde har tilknytning til.



www.biq.dk: Tjenesten BiQ samler oplysninger om virksomheder og personer. Det koster penge at søge, men du kan oprette et prøveabonnement og søge gratis i en uge. Indtast navnet i feltet **Find personer og firmaer (18)** øverst i højre hjørne, og klik på **Søg (19)**. Når du har fundet frem til personen, kan du klikke på knappen **Netværk** for at se, hvem han har tilknytning til.

Hvad laver han ellers?

Efter alle disse kig ned i databaser og registre vender vi blikket ud mod det store, åbne internet. Her regerer søgemaskinerne, som registrerer information på offentligt tilgængelige websider. Den mest kendte søgemaskine er Google, og den er et godt sted at starte. Vi indtaster vores persons navn og sætter anførselstegn foran og bagved. På den måde sikrer vi, at vi kun får søgeresultater om Arne Stahlson – og ikke om sider, hvor der fx et sted står Arne Jensen og et andet står Birgit Stahlson.

Google-søgningen vil sandsynligvis give en række resultater. Hvis Arne Stahlson har en hjemmeside, vil den dukke op her. Det samme gælder andre websider, hvor hans navn står. Det kan fx være en sportsklub, hvor han har deltaget i et mesterskab.

Derimod er Google mindre god til databaser. Der vil således ikke optræde mange af de oplysninger, du kan finde via Den Offentlige Informationsserver, Statstidende og Infomedia. Du kan med fordel supplere Google-søgningen med andre søgemaskiner som Yahoo! **(www.yahoo.dk)** og Live Search **(www.live.com)** fra Microsoft.



www.google.dk: Med Google kan du finde websteder, hvor personens navn optræder. Indtast navnet – med anførselstegn foran og bagved – i søgefeltet **(20)**, og klik på **Google-søgning (21)**. Det kan også være, at Google er stødt på billeder af personen på nettet. Klik på **Billeder (22)**, og se, om der dukker noget op. Men Google tilbyder ikke kun søgning i websider. Internettet har et stort debatsystem, som kaldes Usenet. Ved at søge under Google Grupper – klik på **Grupper (23)** øverst på **www.google.dk** – kan du finde ud af, om Arne Stahlson har haft indlæg her. Databasen går tilbage til starten af 1980'erne.

>>>

Beskyttede data

Der findes også websteder med oplysninger om dig, som er beskyttet mod uvedkommende adgang. I praksis betyder det, at du skal logge ind med brugernavn og adgangskode eller en digital signatur for at se dem. Vi har ikke taget dem med i oversigten her, da formålet er at vise al den information, der er tilgængelig for alle. Men hvis du har en digital signatur, kan du se flere oplysninger om din ejendom i Bygnings- og Boligregistret på www.ois.dk. Du kan også se, hvad CPR-registret (www.cpr.dk) har registreret om dig.

Blev fyret efter Google-søgning

En dansk mand blev tidligere i år fyret fra et nyt job, inden hans prøvetid var ovre. Han syntes ellers selv, at det var gået fint i jobbet. Men arbejdsgiveren fortalte, at han havde søgt efter den ansattes navn på Google. Her havde han fundet en fire år gammel artikel, hvor manden fortalte om sine erfaringer som ludoman. Han er i dag helbredt og er ude af ludomanien. Artiklen stammede fra dagbladet Information. Chefredaktør Palle Weis herfra har fortalt, at Information har fået fem-ti henvendelser fra mennesker, der ønsker, at deres navn fjernes fra artikler i arkivet. Avisen arbejder nu på at udvikle et sæt retningslinjer for, hvordan den skal behandle den slags ønsker.

Hvad siger loven?

Persondataloven bestemmer, hvordan virksomheder og myndigheder skal behandle personoplysninger. Den siger blandt andet, at virksomheder ikke må videregive oplysninger om en forbruger til en anden virksomhed med henblik på markedsføring, medmindre forbrugeren har givet lov til det. Personnumre må kun offentliggøres, hvis personen giver sit samtykke til det.

Loven siger også, at når nogen indsamler personoplysninger, skal de oplyse formålet, hvad oplysningerne vil blive brugt til, og hvordan man kan få indsigt i de data, de indsamler.

Generelt kan du altid få at vide, hvad en virksomhed eller myndighed har registreret om dig. Du kan også gøre indsigelse, hvis du ikke vil have, at de behandler data om dig. Datatilsynet fører tilsyn med, at reglerne i persondataloven overholdes.

Hvor social er han?

Mange danskere er de senere år blevet aktive på sociale netværk som LinkedIn, MySpace og Facebook. I nogle tilfælde kan de almindelige søgemaskiner finde sider på disse netværk, men det er mere sikkert at søge i den enkelte tjeneste. For erhvervsfolk er LinkedIn et oplagt valg, mens yngre mennesker i højere grad er at finde på Facebook. For at få de bedste muligheder for at søge og komme i kontakt med folk skal du i de fleste tilfælde selv oprette dig som bruger på tjenesten.

www.facebook.com:
Det kæmpestore sociale netværk Facebook, hvor millioner af mennesker deler stort og småt fra deres hverdag, lader dig søge efter personer. Du får besked, hvis de kender nogen, som du selv kender. For at komme i gang med at lede efter personer via Facebooks søgefelt **(24)** skal du dog først oprette dig som bruger.

www.linkedin.com:
LinkedIn er et socialt netværk, der især bruges af erhvervsfolk. Her kan du søge i feltet **Search for someone by name** **(25)** og klikke på **Go** **(26)** uden at være oprettet som bruger – men hvis du vil se detaljer om personen, skal du selv oprettes.

Sådan beskytter du dine data
Efter vores rundtur blandt databaserne har du måske fået lyst til at begrænse, hvad andre kan finde om dig. Nogle data kan du kontrollere, men andre kan du ikke gøre noget ved.

Du kan henvende dig til din kommune og få navne- og adressebeskyttelse. Det beskytter dig mod, at Det Centrale Personregisters (CPR) oplysninger om dig bliver givet til private eller optaget i lokalvejvisere. Du kan også få beskyttelse mod henvendelser i forbindelse med statistiske og videnskabelige undersøgelser og markedsføringsbeskyttelse, og via dit telefonselskab kan du få hemmeligt nummer, så du ikke kan findes på fx De Gule Sider.

Oplysningerne om din ejendom i den offentlige ejendomsvurdering og BBR kan du ikke holde hemmelige. Det samme gælder oplysninger i Statstidende, som er offentligt tilgængelige. Du kan som regel heller ikke få fjernet artikler om dig selv i Infomedia.

Når det gælder websteder, har du heldigvis bedre muligheder for at styre informationsstrømmen. Du kan helt lade være med at oprette dig som bruger på Facebook og lignende tjenester. Alternativt kan du oprette dig med et minimum af oplysninger. Men vær opmærksom på, at nettet har en god hukommelse: Når en information først har stået på en webside, kan den være registreret af søgemaskinerne. Selv om du senere sletter den, vil andre måske stadig kunne finde den.

Indlæg på diskussionsgrupperne i Usenet (også kendt som Google Grupper) kopieres automatisk rundt mellem mængder af servere. Det er i praksis umuligt at fjerne et indlæg fuldstændigt fra dem.
Det bedste råd lyder derfor: Brug nettet, og hav masser af glæde af det – men tænk dig altid om, før du lægger informationer om dig selv derud. Det er nemt at lægge informationer ud på nettet, men du skal kunne stå ved det, også om mange år.

Vidste du det? Du kan nemt undersøge, om en person er forfatter eller måske endda komponist. Lav bare en søgning i punktet Forfatter på hjemmesiden www.bibliotek.dk – den omfatter ikke kun bøger, men også artikler i tidsskrifter, noder, dvd'er og musik-cd'er.

Pas godt på dine dyrebare filer



Med USB-nøglen DataTraveler BlackBox fra Kingston er dine filer altid i sikkerhed – også når du er på farten.

Vind supersikre USB-nøgler

I år har der været mange uheldige og pinlige situationer, hvor myndigheder og virksomheder har tabt kritiske persondata. Især i Storbritannien har uheldet været ude, og både myndigheder og banker har simpelt hen tabt cd'er med persondata på flere millioner mennesker. Men selv om uheldet skulle være ude for dig, og du taber dine filer, så kan du nemt sikre dig, at ingen får adgang til dem – du skal bare sørge for at kryptere dem.

Vi udlodder derfor 10 af Kingstons sikre DataTraveler BlackBox USB-nøgler med 2 GB plads (værdi 600 kroner pr. stk.) blandt de rigtige svar på nedenstående spørgsmål. BlackBox-nøglen beskytter dine filer mod, at de forkerte personer får adgang til dem, med en stærk 256-bit hardware-kryptering og har fået den anerkendte FIPS-certifering for sikkerhed. Ud over krypteringen beskyttes dine filer også mod vand og stød af nøglen, der er belagt med titanium og vandtæt i over en meters dybde. Vi udlodder tre grønne, tre røde og fire sorte nøgler på 2 GB.

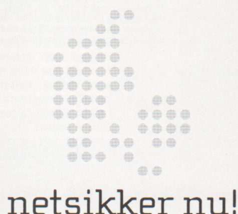
Besvar spørgsmålet, og deltag i konkurrencen om en af de 10 DataTraveler BlackBox USB-nøgler fra Kingston:

Hvor mange bit krypteres data med på Kingstons DataTraveler BlackBox?

A) 56 bit B) 128 bit C) 256 bit

Skriv det rigtige svar i emnelinjen på en e-mail, og send den til **konkurrence@netsikkernu.dk** – og skriv dit navn og din adresse i selve mailen, så vi ved, hvor vi skal sende præmien til, hvis du vinder. Alle vindere vil få direkte besked. Sidste frist for deltagelse er den 31. oktober 2008.

Samarbejdspartnere i netsikker nu! 2008



Arto • Ballerup Bibliotek • BullGuard • Cyberhus • Dansk Metal • Danske Bank • Discus Communications • Ernst & Young • F-Secure • Finansrådet • Forbrugerrådet • Frederikssund Kommune • Gamingschool • Getitcard • Gladsaxe Bibliotekerne • GoSupermodel • Habbo Hotel • Høng Senior Service • IT- og Telestyrelsen • Kaspersky Lab • Komputer for alle • Københavns Biblioteker • Medierådet • Microsoft • Nordea • Parkegaard og Kristensen • Senior IT • Spywarefri • StoneAds • TDC • Transparan-C • Trust Pilot • Uni-C • Websense • Ældremobiliseringen • Ældre Sagen

Hvad er netsikker nu?
Videnskabsministeriet afvikler i samarbejde med en lang række virksomheder og organisationer hvert år kampagnen netsikker nu! Kampagnen sætter fokus på aktuelle it-sikkerhedsproblemer, som vi kan risikere at møde i vores færden på internettet, og formålet er at give gode råd om sikker adfærd på internettet. Kampagnen udmøntes i en lang række kampagneaktiviteter, undervisning, seminarer og materialer. Læs meget mere om netsikker nu! på **www.netsikkernu.dk**

Giv din pc et serviceeftersyn
Som en del af netsikker nu!-kampagnen har TDC sammen med Finansrådet produceret en webside, hvor du kan blive klogere på netsikkerhed, få hjælp til et sikkerhedstjek af din pc og deltage i spillet, hvor du selv skal prøve kræfter med forskellige sikkerhedstrusler – naturligvis uden at din pc kommer i fare. Giv selv din pc et grundigt tjek på **www.opdaterdinpc.dk**

Undgå at falde for svindlernes mails

Hvis en mail lokker med lettjente penge, stammer de gerne fra kriminalitet. Her kan du se, hvordan du genkender en såkaldt phishing-mail, og hvordan du slipper for at ryge i kløerne på svindlere. Af Torben B. Sørensen

"Hjælp os med at hjælpe vores udenlandske kunder. Du får 20 procent af de beløb, du hjælper os med at overføre på vegne af vores klienter."

Har du fået en mail med et tilbud, der ligner ovenstående? Så er du blevet inviteret til at blive medskyldig i hvidvaskning af sorte penge. Svindlen fungerer på denne måde: Nogle forbrydere hacker sig ind på en netbank eller misbruger et kreditkortnummer, de har fået fat i. De overfører pengene til en konto, som du har oprettet. Du hæver pengene, beholder en procentdel og sender resten med en international pengeoverførselstjeneste til udlandet.

Hvis du ikke ønsker at løbe risikoen for en straffesag, er det klogest at slette den slags mails, så snart du modtager dem.

Måske har du også fået en mail af denne type: "Der er fundet et sikkerhedsproblem med din konto her i banken. Vi skal derfor bede dig gå ind og indtaste dine kontooplysninger for at bekræfte dem. I modsat fald bliver vi nødt til at lukke kontoen inden 48 timer. Klik på dette link for at bekræfte dine oplysninger:"

Også her står der med sikkerhed svindlere bag. Linket i mailen fører nemlig ikke til din banks websted, men til en ofte ganske vellignende forfalskning af hjemmesiden. Hvis du indtaster fortrolige data på websiden, lander de hos svindlere, som derefter kan misbruge dem. Den form for svindel kaldes "phishing" – og formålet er at få adgang til fortrolige personoplysninger, typisk kreditkortnumre og kodeord til nettjenester.

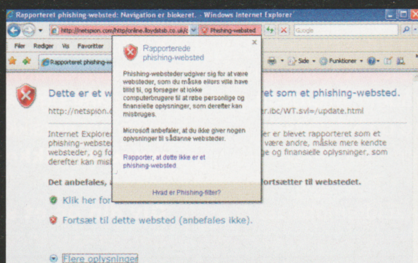
Sådan genkender du phishing

En phishing-mail indeholder altid et link til et websted. Ofte er linket forklædt: Der står måske, at det fører til www.bank.dk. Men hvis du holder musen hen over linket i fx Outlook Express eller Windows Mail, kan du i statuslinjen se, at det i virkeligheden fører et helt andet sted hen.

Hvis du følger disse fire gode råd, er du godt beskyttet mod at blive offer for phishing:

- Undlad at følge links i mails. Hvis du får en mail, der angiver at komme fra din bank, skal du i stedet gå ind på bankens websted via et bogmærke eller ved at indtaste adressen.
- Brug et mailprogram med beskyttelse mod phishing.
- Brug en nyere browser. De nyeste udgaver af Internet Explorer, Firefox og Opera indeholder alle en funktion, der kender en række forfalskede websteder og advarer, hvis du prøver at besøge dem.
- Brug en værktøjslinje, der holder øje med dine internetsider for dig. Firmaet Netcraft og flere andre tilbyder værktøjsbjælker, som du kan installere i din browser. De advarer, hvis du prøver at gå ind på et kendt svindelsted. Netcraft Toolbar giver også en vurdering af, om et websted virker tilforladeligt, idet den blandt andet ser på, hvor længe det har eksisteret. På næste side viser vi dig, hvordan du bruger den.





Phishing-filteret i Internet Explorer 7 advarer, når du er på vej hen til et websted, der er kendt for at blive brugt til phishing-svindel. Dette websted ligger på adressen netspion.com, men svindlerne har forsøgt at få det til at se ud, som om det tilhører banken Lloyds TSB.

Phishing-mails er som regel på engelsk. Nogle få har dog været rettet mod nordiske banker som her Nordea. Men angrebet vil ikke virke, da danske netbankers sikkerhed bygger på mere end brugernavne og kodeord. Svindleren skal også skaffe sig adgang til den såkaldte signaturfil på pc'en, før han kan hacke sig ind på en konto.
Kilde: Version 2



NatWest

National Westminster Bank We are pleased to inform you that the United Kingdom Congress Passed on and signed into LAW the Economic and Growt
Long-Term Tax Relief for all Americans who Pay I
Tax Relief in 2008 and Long Term Tax Relief for t
norminated banks to be Part of the Immediate Ta
Deposit in the Amount of £50,000 in a few Weeks
your Natwest account immediately . Your Amount
the 2000 Federal Tax Return and is just the First I
New Law. The Amount of the Direct Deposit Trans
Debt you may Owe, such as Past Due Child Suppo
no Additional Steps. Your Direct Deposit Transfer
Required to report the Amount as Taxable Income
this Notice with your Tax Records., you are advise
remittance of Funds into your Bank Accounts.

To confirm your identity and to aviod delay kindly take few step to complete the processess. please following the link below to complete.

Log in

National Westminster Bank is committed to ensure the safeguard of each customer's personal information, making sure only authorised individuals have access to their accounts. It is all about your security.

En phishing-mail, der angiver at komme fra banken NatWest. Et klik på knappen Log in fører til et forfalsket websted.
Kilde: millersmiles.co.uk

Accessibility | Legal Info | Privacy Policy | Security | Got a question? Help

NatWest

OnLine Banking
LOG OUT

Restart Log In
Log Out

OnLine Banking

Log In - Step 1

Your Customer Number

Please enter your Customer Number. This is your date of birth (ddmmyy) followed by your unique number which identifies you to the Bank.

Customer number

Forgotten your customer number?

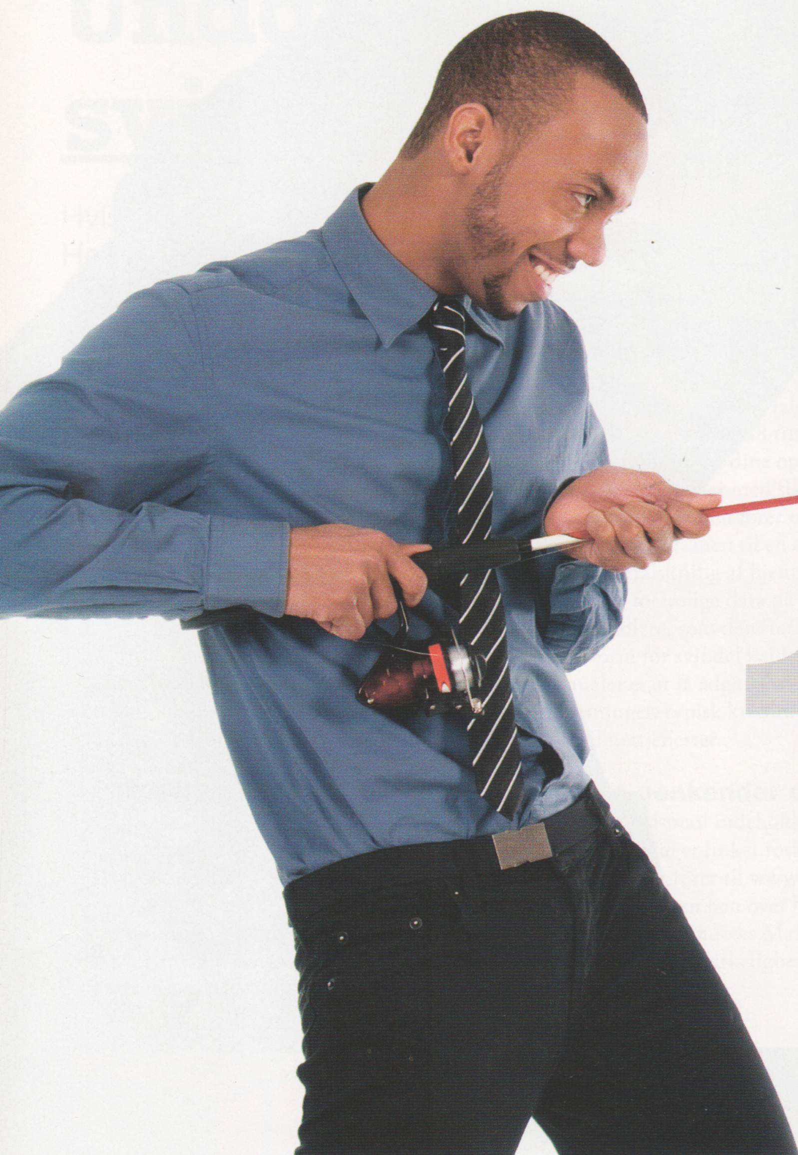
Customers With A New Activation Code

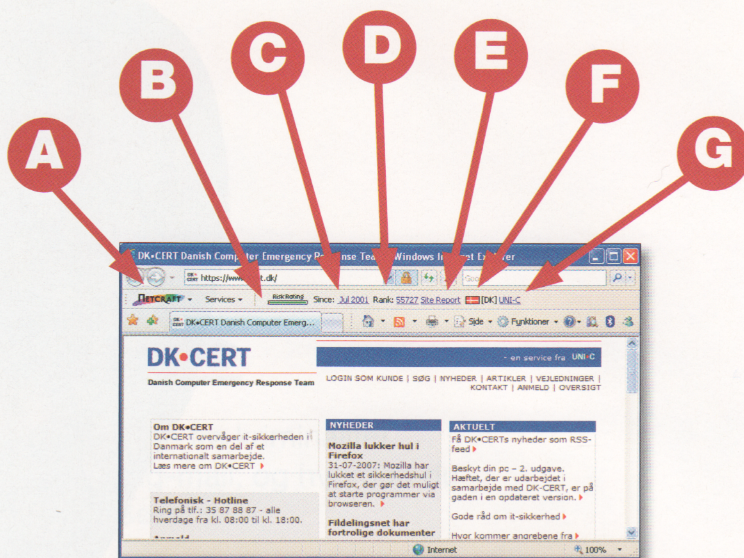
If you have an Activation Code please select this box.

Only individuals who have a NatWest account and authorised access to OnLine Banking should proceed beyond this point. For the security of customers, any unauthorised attempt to access customer bank information will be monitored and may be subject to legal action.

Next

På dette falske websted forsøger svindlere at narre ofre til at indtaste detaljer om deres bankkonto hos NatWest.
Kilde: millersmiles.co.uk





Sådan bruger du Netcraft Toolbar:

1. Hent og installer Netcraft Toolbar. Når programmet er installeret, dukker det op som en værktøjsbjælke i din browser.

A Netcraft-knap. Giver adgang til en række funktioner.

B Risk Rating. Risikovurdering for det websted, browseren viser.

C Since. Første tidspunkt, hvor Netcraft har registreret data om webstedet.

D Rank. Popularitet blandt alle websteder, som Netcraft følger.

E Site Report. Rapport om webstedet.

F Flag. Det land, hvor webserveren er registreret.

G Netblock. Ejeren af webserverens IP-adresse.

Beskyt dig mod phishing med Netcraft Toolbar

Hvis du vil supplere den indbyggede phishing-kontrol i browseren Internet Explorer 7, kan du installere Netcraft Toolbar. Firmaet Netcraft vedligeholder en liste over servere, der er kendt for at huse phishing-svindel i form af forfalskede websteder. Når du prøver at gå ind på et websted, sammenligner Netcraft Toolbar dets adresse med listen. Hvis adressen optræder på listen, bliver du advaret mod at besøge det. Find linket til, hvor du gratis kan hente Netcraft Toolbar, på **www.komputer.dk/netsikker**

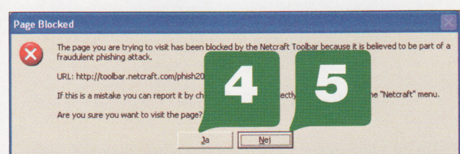


2. Indtast adressen på et websted i **adresselinjen (1)**, og tast **Enter** på tastaturet. Netcraft Toolbar giver nu oplysninger om det websted, du har valgt. Den vigtigste er risikovurderingen. Sikre websteder vises med grønt, mens usikre markeres med rødt. Dog vil et nyoprettet websted, som Netcraft ikke kender, altid være markeret med rødt, skønt det kan være helt ufarligt.

3. Hvis du vil vide mere om et websted, kan du klikke på knappen **Site Report**. Punktet **Organisation (2)** fortæller, hvem der har registreret webadressen. Hvis det er en anden end den, du havde ventet, kan det være tegn på forfalskning. I mange tilfælde lader firmaer dog samarbejdspartnere registrere adresser, så der er ikke nødvendigvis noget galt. Under punktet **Date seen first (3)** kan du se, hvor længe websiden har eksisteret.



4. Hvis du prøver at besøge et websted, som Netcraft har registreret som farligt, får du nedenstående advarsel. Klik på **Ja (4)**, hvis du vil besøge hjemmesiden på trods af advarslen, og **Nej (5)**, hvis du ikke ønsker at åbne den alligevel.



Mand fra Næstved blev muldyr for netsvindlere

I efteråret 2006 modtog en mand i Næstved en mail fra et udenlandsk investeringsfirma. De indbød ham til et forretningssamarbejde. Han skulle oprette en konto, som de kunne overføre penge til. Når de fik brug for hans hjælp, skulle han hæve pengene og sende dem via pengeoverførselstjenesten Western Union. Som tak for ulejligheden kunne han beholde en del af pengene.

Manden kontaktede sin bank og SKAT for at sikre sig, at der ikke ville være noget problem i at oprette kontoen og starte samarbejdet. Han rådførte sig også med sin revisor, fordi det var en ny type forretning for ham, og han ville vide, hvordan han skulle bogføre indtægterne. Derefter oprettede han kontoen, og den 12. december 2006 blev der overført 61.396 kroner til hans nye konto. Han hævede pengene og sendte 44.958 kroner til en modtager i Rusland.

Da der et par dage efter igen kom penge ind på hans konto, gik han i banken for at hæve dem. Men nu ventede politiet på ham. De tog ham med, og han blev tiltalt for hæleri. De penge, der var blevet overført til hans konto, tilhørte nemlig ikke investeringsfirmaets klienter, men kom i stedet fra danske bankkonti, som ukendte gerningsmænd havde hacket sig ind på. Men da det er svært at overføre penge til udlandet fra en netbankkonto uden at efterlade sig spor, havde bagmændene hyret manden som hjælper. I branchen kalder man den slags for "muldyr." Hans opgave var at hvidvaske pengene: Når han hævede dem og derefter sendte dem via Western Union, var der intet spor fra de hackede bankkonti til bagmændene i Rusland.

Var i god tro

Sagen kom for retten i efteråret 2007. Ingen var i tvivl om, at pengene var tilvejebragt ved forbrydelser. Men retten mente, at manden måtte have været i god tro – han havde rådført sig med både banken, skattevæsenet og sin revisor. Derfor blev han frifundet. Hans forsvarer, advokat Jørgen Damgaard, siger om udfaldet af sagen:

"Dommen betyder ikke, at der er grønt lys for at gøre den slags fremover. I den type sager vil det altid være en konkret vurdering i hvert enkelt tilfælde, om den tiltalte har været i god tro. Generelt vil jeg sige, at hvis der er tale om lettjente penge, skal man altid være på vagt. Som regel skyldes den nemme gevinst, enten at man løber en stor risiko, eller at det er ulovligt. Og da man i disse sager får pengene ind på sin konto, før man skal sende dem videre, løber man ingen risiko..." siger han.

Muldyr blev dømt

Andre sager viser, at det kan være strafbart at agere muldyr. I december 2007 blev en ukrainsk mand ved retten i Kolding idømt 60 dages fængsel og udvisning, efter at han havde skaffet russiske gangstere 69.000 kroner. Han havde stillet en bankkonto til rådighed for dem.

I januar 2008 blev en 26-årig dansker ved Vestre Landsret idømt et halvt års fængsel eller 150 timers samfundstjeneste. Han havde modtaget 315.000 kroner fra hackede netbankkonti i danske banker. Her var pengene sendt videre til en konto i Dubai. Landsretten mente, at fremgangsmåden lugtede så meget af svindel, at den tiltalte burde have indset, at der var tale om ulovligheder.

Phishing: Svindel, der går ud på at lokke fortrolige oplysninger som fx kreditkortnumre fra ofrene. Kommer af det engelske ord "fishing" (fiskeri), fordi svindlerne prøver at fiske informationer fra folk.

Muldyr: Et "muldyr" er leddet mellem offeret for et netbankindbrud og de svindlere, der ønsker pengene overført til udlandet. Pengene fra indbruddet overføres til muldyrets konto, og muldyret instrueres i at hæve beløbet i kontanter og sende pengene ud af landet via pengeoverførselsfirmaer som fx Western Union. Muldyret får lov til at beholde en andel af beløbet for "ulejligheden".

Vidste du det? En elektronisk bankoverførsel, som bliver brugt i disse svindelnumre, kan altid spores – og derfor er der 100 % opdagelsesrisiko for muldyrene, som politiet altid finder frem til, fordi det er deres bankkonti, der bliver brugt.

Gå i banken hjemme fra sofaen

Omkring tre millioner danskere bruger nu netbank på deres computer i stedet for at stå i kø i banken. Det er nemt og hurtigt – og så er sikkerheden i top. Af Chris Hansen

Flere og flere har fået øjnene op for, hvor smart det er bruge netbank på hjemme-pc'en. Ud over at blive fri for turen til banken slipper man nemlig også for en meget stor del af de sædvanlige bankgebyrer ved at klare arbejdet selv. Der er nærmest ingen grænser for, hvad man kan ordne hjemmefra i ro og mag, og det er netop mageligheden ved netbanken, der i stigende grad lokker danskerne hen foran skærmen, mener Martin Andersen, der er chef for Nordeas netbank.

"Du kan handle aktier i netbanken, indbetale girokort, ansøge om lån og kommunikere med din rådgiver, når det passer dig," siger han.

Den store stigning i antallet af danskere, der bruger netbank, har gjort den ellers normalt så stille søndag til en af de helt store bankdage. Når ugens ræs er overstået, klares bankforretningerne hjemme på arbejdsværelset eller fra den bærbare pc i sofaen.

Brug trygt din netbank

I dag er det faktisk stort set kun nødvendigt at besøge banken, hvis du vil hæve kontanter eller deponere værdier i en bankboks, og alder er ingen hindring for at klare bankforretningerne selv – det kræver blot en computer med adgang til internettet.

"Engang var det kun de unge, der brugte netbank," fortæller Martin Andersen, "men i dag er størstedelen af brugerne over 50 år, og vi har sågar kunder på 90, der bruger netbank."

Og sikkerheden i netbanken er mindst lige så høj, som hvis du besøger din almindelige bankfilial. Det kan ikke lade sig gøre at bryde ind i netbanken hos banken, men rent teknisk kan en svindler dog godt overtage kontrollen over din computer og på den måde få adgang til dine konti. Du kan dog nemt selv undgå indbrud ved at opdatere din computer med de seneste opdateringer til Windows, den nyeste antivirus og en firewall. Det kan endda gøres ganske gratis, hvilket du kan læse mere om andetsteds i dette magasin. Skulle det utænkelige alligevel ske – at en tyv får adgang til netbanken og overfører penge til sin egen konto – så dækker banken tabet.

Blandt de tre millioner danskere, som har netbank, var der kun 85 tilfælde af indbrud i netbanken sidste år, oplyser Finansrådet. Til sammenligning var der ifølge Danmarks Statistik mere end 36.000 indbrud i de godt 2,5 millioner danske husstande.

10 gode råd om at undgå internetsvindel

1. Brug et antivirusprogram, der opdateres automatisk og altid er slået til.

2. Anvend en personlig firewall på computeren.

3. Installer løbende sikkerhedsopdateringer til din software.

4. Slet spam uden at læse det.

5. Åbn ikke vedhæftede filer, og klik ikke på links i mails, medmindre det er en mail og en fil, du har ventet.

6. Indstil sikkerhedsniveauet i din browser, så du altid bliver spurgt, når informationer, filer og programmer overføres til din computer.

7. Undlad at reagere på uopfordrede mails, hvor du bliver bedt om at indtaste følsomme oplysninger.

8. Hent ikke programmer fra internettet, medmindre du stoler på det website, du henter dem fra.

9. Anvend kryptering, hvis du installerer trådløst netværk.

10. Tag løbende sikkerhedskopier af dine filer.

Mener du, at din pc er angrebet, så vent med at bruge din netbank, til pc'en er bragt i orden. Hvis din pc allerede er inficeret af en virus, og du efterfølgende har anvendt netbanken, så kontakt straks banken for at spærre netbanken.
Kilde: Finansrådet

Vidste du det? De fleste banker tilbyder en telefonservice, hvor medarbejdere sidder klar til at hjælpe dig med at holde din computer sikker og hjælpe dig med din netbank. Læs mere på din banks hjemmeside eller i de papirer, du fik, da du oprettede din netbankaftale.



"Engang var det kun de unge, der brugte netbank, men i dag er størstedelen af brugerne over 50 år, og vi har sågar kunder på 90, der bruger netbank," siger Martin Andersen, der er chef for Nordeas netbank.

Sikker betaling med Dankort på nettet

Ud over netbank kan du også handle med dit Visakort eller Dankort på internettet, og hver eneste dag skifter rigtig mange penge hænder på den måde. PBS, der styrer internetbetalinger i Danmark, har opgjort antallet af betalinger til mere end 8,3 millioner i 2. kvartal af 2008 alene.

Betaling med Dankort på internettet er lige så nemt som netbank, og sikkerheden er høj. Dukker varen ikke op, så kan du bede banken tilbageføre alle pengene. Har du derimod forudbetalt en vare med girokort, bankoverførsel eller check, og varen ikke dukker op, så kan pengene være tabt, og derfor anbefaler Forbrugerombudsmanden, at man så vidt muligt handler med betalingskort på nettet. Forbrugerombudsmanden råder dog også til, at man er varsom med, hvem man udleverer sit kortnummer til. Nogle danske hjemmesider har det såkaldte e-mærke, der markerer, at her er det trygt og etisk forsvarligt at handle. På udenlandske hjemmesider er e-mærket ikke til stede, og så må man bruge sin gode forstand til at afgøre, om det er sikkert at handle med sit betalingskort.

Læs om køb af varer på internettet på Forbrugerstyrelsens hjemmeside: **http://www.forbrug.dk/raad/naardukoeber/ehandel/**

Antivirus: Et antivirusprogram er et program, som ligger i baggrunden og holder øje med de andre programmer, der kører på din pc. Hver gang du fx åbner et program eller læser en mail, tjekker antivirusprogrammet, om programmet eller mailen indeholder nogen af de virus, som det kender. Når du installerer et antivirusprogram, vil det normalt som det første tjekke hele din harddisk for virus.

Firewall: En firewall er et program eller en særlig computer, der bruges til at sikre computerne på indersiden af firewallen mod angreb (fx fra hackere) fra den ydre verden. Firewallen bruger såkaldte portnumre til at afgøre, om en pakke med data skal have adgang til din computer – og som regel tillader en firewall kun indkomne pakker, der er svar på henvendelser, som pc'en selv har afsendt.

Godt i gang med netbank

Først og fremmest skal du bruge en pc med internetforbindelse, men for at komme i gang med at bruge netbank skal du som regel ind i en bankfilial og bestille en aftale hos din bankrådgiver. Men tænk: Det kunne være sidste gang, du står i kø ved kassen. Netbanken koster ikke noget. Fremgangsmåden er forskellig fra bank til bank (der følger som regel en grundig vejledning med i det materiale, som banken udleverer), men i de fleste tilfælde får du en kode, som du skal bruge. Inden du går i gang foran skærmen derhjemme første gang, skal du sikre dig, at du har opdateret softwaren på din computer. Læs mere om det andetsteds i magasinet. Du navigerer i netbanken via din sædvanlige internetbrowser (Internet Explorer, Firefox eller lignende), og bankforretningerne kan nemt klares med selv de langsomste internetforbindelser.



10 gode råd, når ungerne går online

Internettet er kommet for at blive. Og mens forældre kan være skeptiske, er dagens børn og unge indfødte på nettet. Derfor kommer du meget længere med et godt råd og en voksen erfaring end med forbud og regler. Af John Alex Hvidlykke

Det kan godt være, at børn for en generation siden kunne nøjes med en cykel og en kasse legoklodser og i øvrigt være tilfredse med det. Men i det 21. århundrede er computere og internet en uundgåelig del af dagligdagen for børn og unge. Så du kan lige så godt vænne dig til tanken – for der er ingen tegn på, at nettet forsvinder i den nærmeste fremtid. Tværtimod.

Når det gælder den tekniske side af sagen, er børn og unge fuldt ud i stand til at klare ærterne selv. Hvad der for forældre kan være skræmmende eller forvirrende ny teknik, er lige så naturligt for børnene som at skifte kanal på fjernsynet. Det handler i stedet om at give den næste generation en god start og nogle gode vaner i omgangen med det nye medie. Og her er der brug for al mulig hjælp fra de voksne: Hvad enten mediet er websider, chatrum eller fjernsyn, er der behov for at være kritisk over for de tilbud, der strømmer ind. Ikke alle er, hvem de giver sig ud for, eller har de hensigter, de påstår – og her er et råd fra en erfaren voksen velkomment. Husk blot, at det mere handler om at dele sine erfaringer end at udstikke regler og forbud. Alt, hvad der er forbudt, vil pr. definition være interessant og en velkommen anledning til at gøre oprør og vise "de gamle", at man sandelig godt selv kan finde ud af det. Sammen med Medierådet for Børn og Unge har vi samlet de bedste råd til forældre, som med bævende hjerte sender afkommet ud på informationsmotorvejen. På næste side viser vi også, hvordan du med programmet Familiesikkerhed fra Microsoft kan sætte nogle generelle grænser for, hvilke sider dine børn må besøge.

1 Skete der noget på nettet i dag?

Det bedste middel mod mystik og misforståelser er at snakke om tingene. Lad børnene fortælle om deres oplevelser ude i cyberspace. Hvilke sider er det, de besøger – og hvorfor er det spændende? Spørg gerne, men husk, at det ikke er et forhør – bare almindelig dialog over aftensmaden.

2 Prøv selv

Hvis du er en af de voksne, som aldrig er kommet med på chat og sms, er det svært at være et meningsfuldt forbillede for børnene. Prøv det selv! Send en sms til børnene i stedet for at ringe og spørge om, hvornår de kommer hjem. Besøg et chatrum. Få dig en karakter i World of Warcraft. Måske er der ikke så meget at frygte i virkeligheden.

3 Du må ikke...

...bare konsekvent udstede forbud! Forbud avler mistro og fører i sidste ende blot til, at børnene gør netop det, du siger, at de ikke må. Vær hellere realistisk, og tal med dem om, hvad der er en rimelig grænse for computerbrug, og hvorfor det måske ikke er en god idé at besøge bestemte sider på internettet eller spille de mest bloddryppende spil.

4 Så hør dog efter!

Hvis du ikke forstår, hvad der foregår i de unges hoveder, er det måske, fordi du ikke lytter til, hvad de fortæller dig! Kom ud af kakkelovnskrogen, læg avisen, og tag filttøflerne af. I virkeligheden vil de unge gerne dele både de spændende oplevelser og de mindre behagelige. Lyt også til, hvad de ikke siger – så du får at vide, hvad der virkelig trykker.

5 Børn nu om dage!

Du er ikke den første forælder i verden, som kan have svært ved at forstå sit afkom. Den slags skete også for de gamle grækere. Og for dine egne forældre. Tal med andre i samme situation, og hør, hvordan de tackler tingene, i stedet for at bakse med dem alene.

6 Træd i karakter

Uanset at al nysgerrighed er godt, skal du ikke være bange for at træde i karakter og sige fra, hvis poderne er på gale netveje. Det er vigtigt at kende forskel på rigtigt og forkert. Så sig nej til ulovlige downloads, "sjove" forsøg med hacking, og hvad du ellers ikke vil acceptere.

7 Hvad synes du selv?

Uanset hvad kan du ikke altid være der, når børnene går på nettet. Så lær dem at bruge deres sunde kritiske sans. Det gælder ikke mindst, når de møder nye mennesker på nettet. Hvad vil du fortælle til en fremmed – og vil du mødes med vedkommende i den virkelige verden?

8 Ud på de vilde vover

Selv om de unges gøren og laden på nettet er totalt urimelig og uansvarlig – så husk, at det hører ungdommen til at afsøge grænserne og finde ud af, hvor man selv står. Og i sidste ende er det sværere at komme til skade på internettet end de fleste andre steder. Du skal blot være klar med et voksent råd, når der senere er brug for et råd fra en, der selv har prøvet det hele for mange år siden.

9 Brug filtre med omtanke

Hvis du vil holde snor i afkommets internetforbrug, kan et filterprogram være løsningen. Et surf-filter kan – ideelt set – give uhindret adgang til alle nettets herligheder, men spærre adgangen til farlige og ubehagelige sider. Desværre er det meget svært at lave et filter, der kan skelne skidt fra kanel og tilmed være så fleksibelt, at det kan give de helt rette sider til både Kenneth på 14 og lille Benjamin på seks et halvt. Brug filtre, hvis du synes, det er nødvendigt, men gør det med omtanke. Hvem kan lide at være under administration?

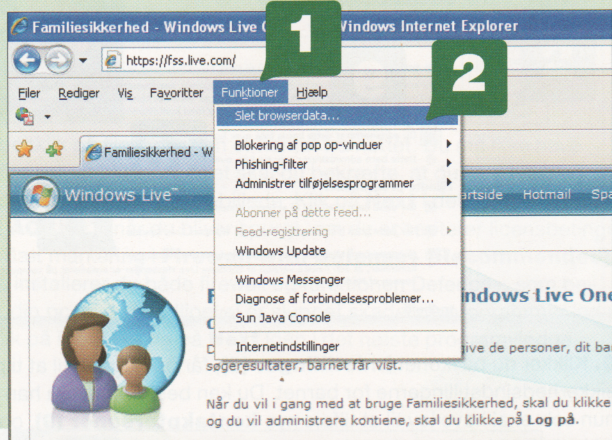
10 Nettet er kommet for at blive

Hvad enten du synes om nettet eller ej, kan du ikke proppe trolden tilbage i æsken. Internettet er en uundværlig del af livet for børn og unge. Biltrafik er også farlig, men vi brækker jo ikke asfalten op af den grund. Lær hellere dine børn at begå sig i trafikken, inden du sender dem ud at lege på den digitale motorvej.

Ryd op efter dig selv!

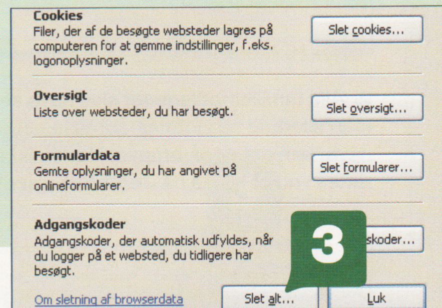
Bare fordi pc'en bruges af alle i familien, betyder det ikke, at alle nødvendigvis har godt af at se de samme websider. Derfor kan det være uheldigt, når Internet Explorer – som en ekstra service – hjælper med at fuldføre de hjemmesideadresser, man er i gang med at indtaste i adresselinjen. Især hvis mor eller far har besøgt sider, der er forbudt for børn.

Og nej, det behøver ikke være sider med såkaldt voksent betalingsindhold. Også nyhedsmediernes sider indeholder filmklip og historier, der bestemt ikke er egnede for unge, vandblå øjne. Løsningen er at sørge for, at Internet Explorer glemmer siderne igen:



1. Åbn Internet Explorer 7, og vælg menuen **Funktioner (1)**. Klik nu på **Slet browserdata... (2)**.

2. Nu kan du vælge, hvilke oplysninger du vil have browseren til at glemme. Jo flere du sletter, desto sikrere – og desto mere er du nødt til at huske selv. Vil du være på den sikre side, skal du vælge **Slet alt... (3)**.



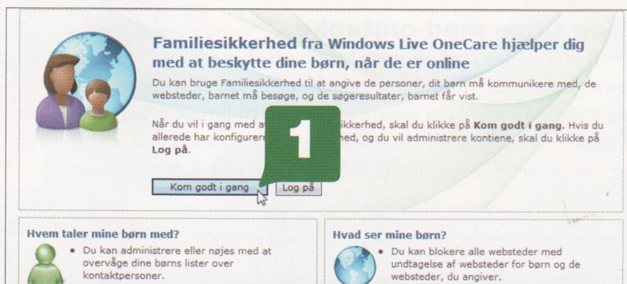
Vidste du det? Cyberhus er et gratis tilbud på nettet, hvor teenagere kan få hjælp til ungdomslivets små og store spørgsmål. Via hjemmesiden www.cyberhus.dk kan børn og unge anonymt chatte med professionelle voksne rådgivere om emner som følelser, venner, mobning, sex, sundhed, tro, sorg, kærlighed mv. og skyde genvej til det gode ungdomsliv.

Windows passer på børnene

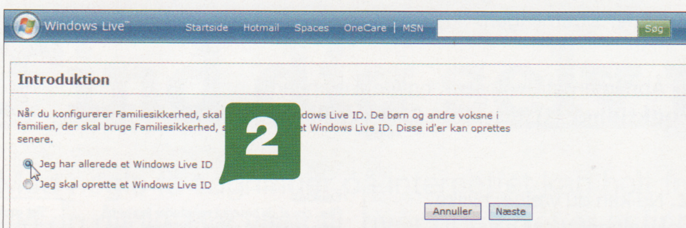
Windows Familiesikkerhed er smart, hvis du ikke er helt tryg ved at slippe børnene løs på nettet.

Programmet er en gratis del af Microsofts programpakke Windows Live, og det kan hentes på Microsofts websted. Når Windows Live Familiesikkerhed er installeret på pc'en, kan kun de familiemedlemmer, der er oprettet i programmet, få adgang til internettet – og kun i det omfang, I som forældre tillader det.

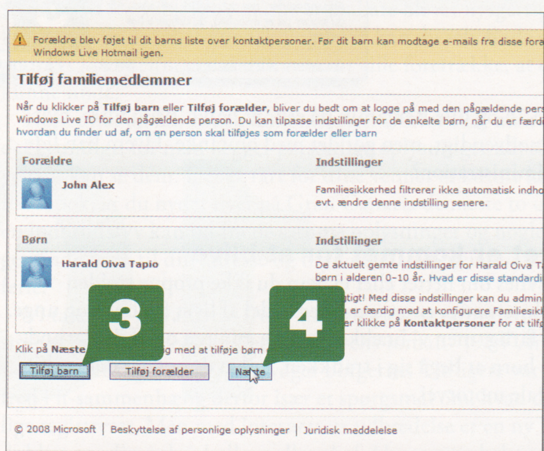
Sådan opretter du Familiesikkerhed



1. Start med at besøge https://fss.live.com, og klik på **Kom godt i gang** **(1)**.



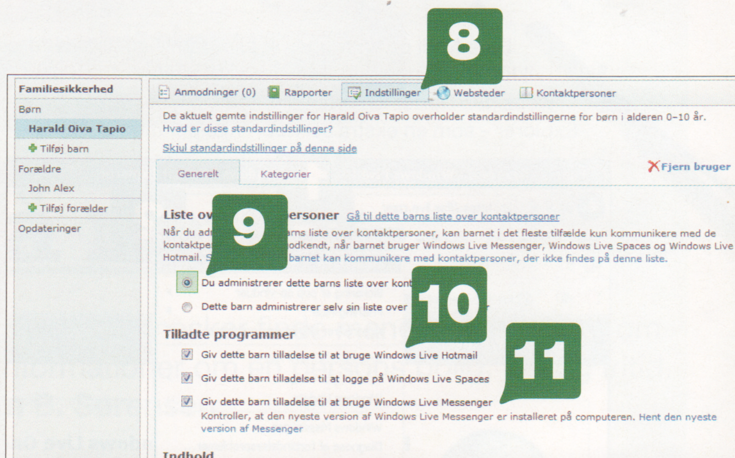
2. Alle familiemedlemmer skal have et såkaldt Windows Live ID. Har man allerede en Hotmail-adresse eller et Microsoft Passport-brugernavn, kan det også bruges. Har du ikke et brugernavn, kan det oprettes ved at klikke på **Jeg skal oprette et Windows Live ID** **(2)**.



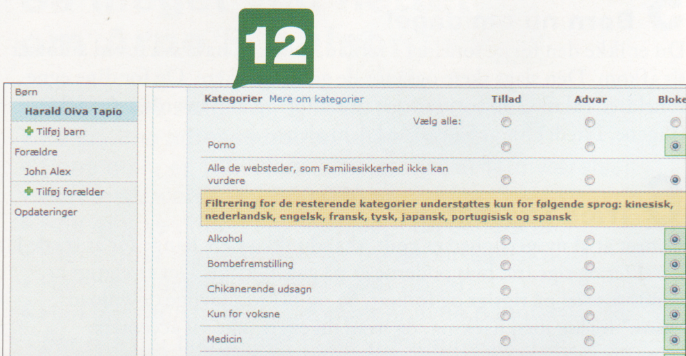
3. På skærmbilledet **Tilføj familiemedlemmer** kan du tilmelde børn og forældre **(3)**. Har de ikke allerede et brugernavn, kan det oprettes på stedet. Klik så på **Næste** **(4)** og derefter på knappen **Hent** for at downloade og installere Familiesikkerhed.



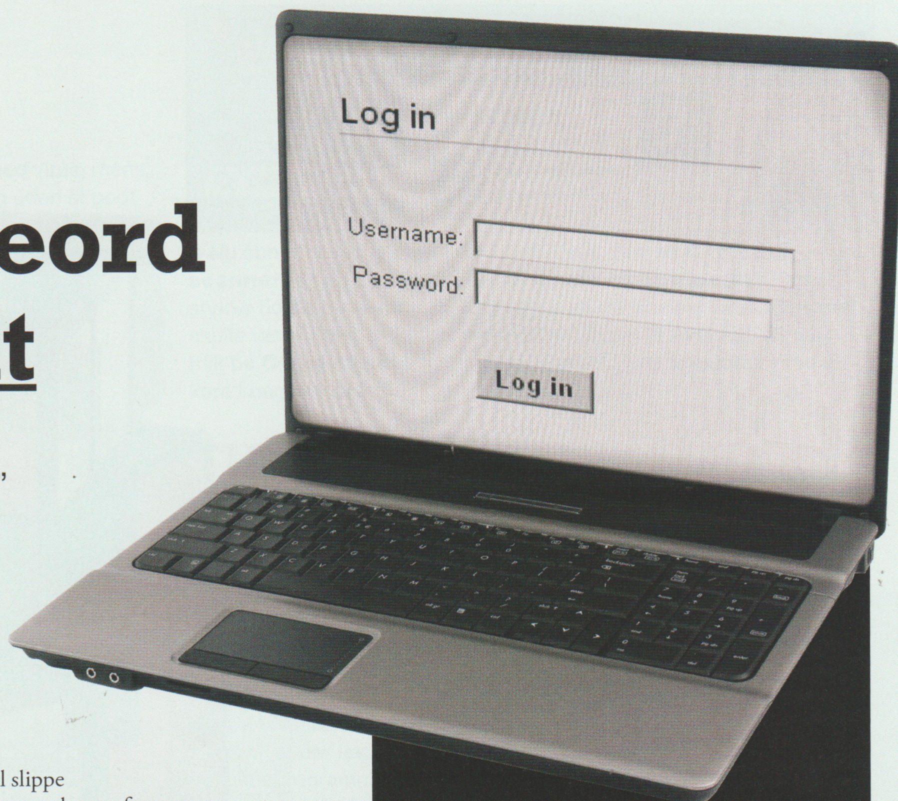
4. Når programmet er installeret, kommer den komplicerede del: Hvad skal tillades, og hvad skal udelades? Det kommer i høj grad an på afkommets alder og familiens værdier. I dette tilfælde vælger vi fx, at den i øvrigt glimrende nyhedstjeneste CNN nok er for hård kost. Vi indtaster www.cnn.com ud for **http://** **(5)** og klikker på **Bloker** **(6)**. Tilsvarende skal du klikke på **Tillad** **(7)**, hvis du vil godkende siden.



5. Klikker du på ikonet **Indstillinger** **(8)**, får du adgang til at tilpasse sikkerhedsindstillingerne for barnet. Du kan bestemme, om han eller hun selv skal have lov til at tilføje nye **kontakptersoner** **(9)**, og kan lukke helt af for Hotmail **(10)** og chatprogrammet Messenger **(11)**.



6. På fanebladet **Kategorier** **(12)** kan du lukke helt eller delvist af for udvalgte typer "plager" på nettet. Tobak, bomber, seksualundervisning, alkohol og mail for blot at nævne nogle. Uhada! Det er dog langtfra alle sider, der kan vurderes automatisk, da filteret fx ikke forstår dansk.



Gør dit kodeord superstærkt

Hvis du hedder Hans Jensen, er det en rigtig dårlig idé at vælge "hans" som brugernavn og "jensen" som adgangskode. Læs her, hvordan du vælger det stærkeste kodeord.

Af John Alex Hvidlykke

Et usikkert kodeord er det digitale sidestykke til at gemme nøglen under dørmåtten. Har du valgt "test" som kodeord, tager det en trænet hacker under et sekund at bryde ind i dit digitale hjem. Hvis du vil slippe for den slags ubehageligheder, er dit vigtigste forsvarsvåben et godt – og først og fremmest originalt – kodeord, som ikke kan gættes af hackerne og deres programmer.

Tr0f@sT er o.k.

Det er et klassisk råd for adgangskoder, at man bør undgå ord, som kan forbindes med en selv – som navnene på børn eller kæledyr eller fødselsdatoer. Dels er der risiko for, at skumle personer, som kender en smule til dig, vil kunne gætte koden, dels prøver moderne hackere sig frem med ordlister med tusindvis af almindelige ord og talkombinationer. Du kan dog sagtens anvende kodeord fra dagligdagen, men sørg for, at du supplerer koden med tal, tegn og store bogstaver – og som absolut minimum bruger seks tegn, men helst flere. Således kan menneskets bedste ven, Tr0f@sT, altså blive et glimrende kodeord.

Jo længere, desto bedre

Et godt kodeord er langt. Jo flere tegn, desto længere tid tager det for en computer at arbejde sig systematisk igennem alle kombinationsmuligheder. Fem tegn er derfor 28 gange bedre end sølle fire tegn, hvis du nøjes med alfabetets bogstaver. Og et bogstav mere gør kodeordet 784 gange stærkere end fire-tegns-koden.

Vælger du et kodeord på 10 bogstaver, er der 296.196.766.695.424 kombinationsmuligheder, men endnu bedre er det dog, hvis kodeordet indeholder både store og små bogstaver samt tal. Så bliver antallet af muligheder astronomisk (eller mere præcist 1.568.336.880.910.795.776!).

Husketeknik

Desværre er det svært for almindelige mennesker at huske et superlangt kodeord med en række helt tilfældige cifre. Det behøver du heller ikke. Kodeordet kan være en forkortelse af en sætning: "I morgen er der atter en dag" bliver fx til det kryptiske "imedaed" eller det endnu sikrere "Imeda1d". Men det er selvsagt en fordel at vælge en mindre kendt sætning som nøgle.

Tjek dit eget kodeord

Du kan selv nemt tjekke, hvor gode dine egne kodeord er. Programmet Tjek dit kodeord er udviklet af magasinet Komputer for alle og vurderer styrken af dit kodeord, lige så hurtigt som du kan taste det ind. Indtast dit kodeord i feltet **Indtast kodeord** **(1)**, og se nedenunder **(2)**, hvor sikkert det er. For at være helt sikkert skal kodeordet indeholde mindst otte tegn, både tal, store og små bogstaver og specialtegn (fx @, £ og $). Det kan dog variere fra sted til sted, hvilke og hvor mange tegn det er tilladt at bruge – så prøv dig frem.

Hent Tjek dit kodeord på **www.komputer.dk/netsikker**

Tjek dit kodeord - Komputer for alle

Tjek dit kodeord

Indtast kodeord: ●●●●●●●●●●● 1 2

Sikkert ☑ Skjul kodeord

Den sikre vej til et godt kodeord:

- ☑ Brug mindst otte tegn
- ☑ Brug både store og små bogstaver
- ☑ Brug tal
- ☐ Brug specialtegn (fx @, !, +, ? med flere)
- ! Brug aldrig dit eget, et familiemedlems eller dit kæledyrs navn – det er for nemt at gætte.

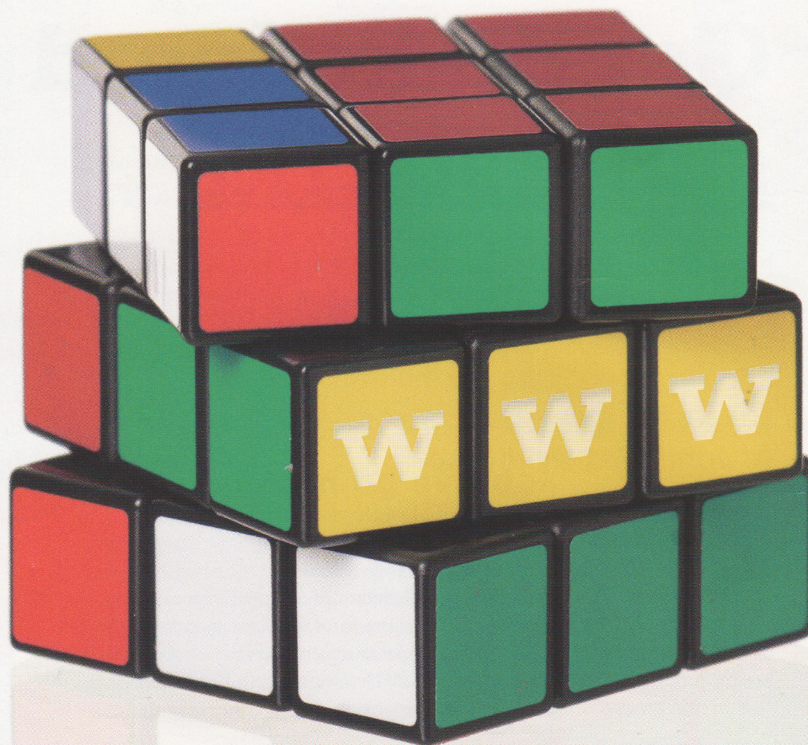
Ikke alle kodeordsbeskyttede sider og programmer understøtter samtlige specialtegn. Det vil du i så fald blive gjort opmærksom på, når du opretter dit kodeord.

KOMPUTER FOR ALLE

Læs meget mere om sikkerhed på www.komputer.dk/sikkerhed

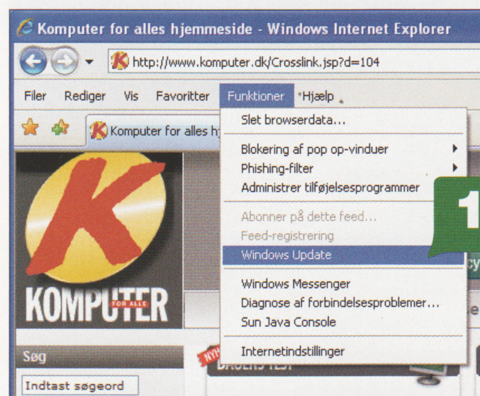
Vidste du det? En engelsk undersøgelse af kodeord i 2006 viste, at originaliteten (og dermed sikkerheden) blandt de adspurgte brugere bestemt ikke var høj. De 10 mest almindelige kodeord i undersøgelsen var: 1. 123 2. Password 3. Liverpool 4. Letmein 5. 123456 6. Qwerty 7. Charlie 8. Monkey 9. Arsenal 10. Thomas

Gør Internet Explorer topsikker



Med nogle få nemme tricks kan du gøre din færden på internettet meget mere sikker – og det hele kan klares i Internet Explorer. Af Torben B. Sørensen

Internet Explorer 7 fra Microsoft er ubetinget verdens mest populære program til at se websider med. Men fordi browseren er så udbredt, er den også et meget populært mål blandt dem, der gerne vil installere skadelige programmer på din computer. Vi viser dig her, hvordan du sikrer din browser.

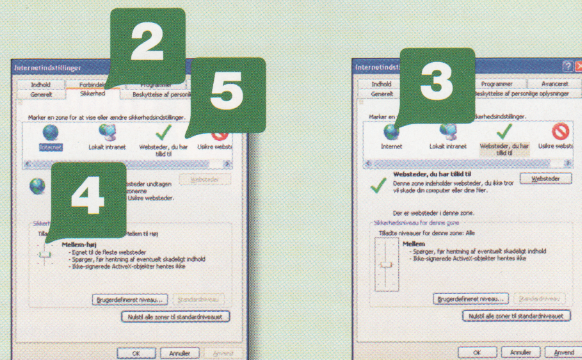


1: Hold Internet Explorer opdateret

Når skadelige programmer og hackere kommer ind på din pc, skyldes det ofte, at de udnytter fejl i Internet Explorer og andre programmer. Microsoft udsender løbende rettelser, der fjerner fejlene, men for at være helt sikker på, at du har alle de nyeste opdateringer, kan du åbne Internet Explorer, vælge menuen **Funktioner** og klikke på **Windows Update (1)**. Hvis menuen **Funktioner** ikke er synlig i din browser, skal du bare trykke på tasten **Alt** på dit tastatur for at få den frem.

2: Vælg et højt sikkerhedsniveau

Internet Explorer opdeler websteder i forskellige zoner – og du kan nemt angive et sikkerhedsniveau for hver zone. Som udgangspunkt befinder alle websteder sig i zonen Internet. Du angiver sikkerhedsniveauet for zonen sådan: Gå ind i menuen **Funktioner**, og vælg **Internetindstillinger**. Klik på fanebladet **Sikkerhed** (2) og derefter på **Internet** (3) for at indstille niveauet. Hvis du vil være meget sikker, skal du trække skydeknappen (4) op til **høj**. Det giver dig stor sikkerhed på pc'en, men medfører også, at mange websteder holder op med at virke. For at få de websteder, som du ofte bruger, til at virke igen skal du flytte dem fra zonen **Internet** til zonen **Websteder, du har tillid til** (5). Klik på zonen og derefter på knappen **Websteder** for at tilføje websteder til den.

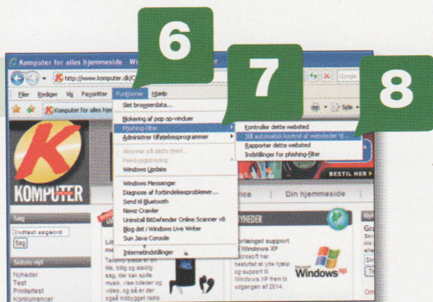


3: Pas på udvidelserne

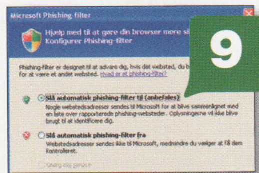
En del af de angreb, der er rettet mod Internet Explorer, udnytter fejl, der faktisk slet ikke ligger i programmet selv. I stedet går de efter fejl og sikkerhedshuller i de udvidelser og støtteprogrammer, som kan startes via Internet Explorer. Det er fx programmer, som viser video, animationer eller andre former for særligt indhold. For at øge sikkerheden kan du begrænse mængden af dem: Sig nej tak, når en webside, som du ikke har fuld tillid til, spørger, om den skal installere en udvidelse. Du kan se de udvidelser, der allerede er installeret i Internet Explorer, ved at gå ind i menuen **Funktioner**, vælge **Administrer tilføjelsesprogrammer** og klikke på **Aktiver eller deaktiver tilføjelsesprogrammer**.

4: Bliv advaret om svindlere

Internet Explorer 7 har en indbygget funktion til at beskytte mod forfalskede websteder, som anvendes til phishing-svindel (forsøg på at lokke personlige oplysninger ud af dig).

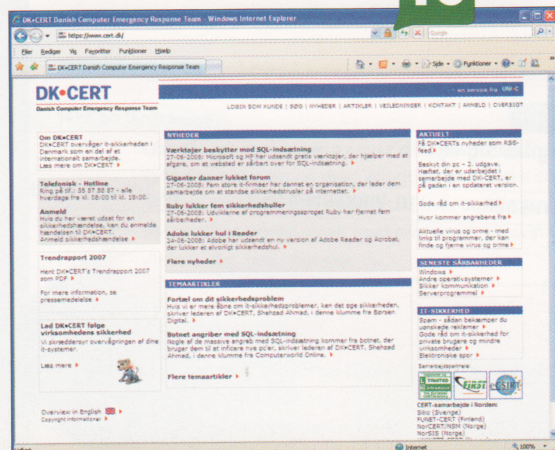


1. Start Internet Explorer. Gå ind i menuen **Funktioner (6)**. Vælg **Phishing-filter (7)**, og klik på **Slå automatisk kontrol af websteder til (8)**.



2. Vælg **Slå automatisk phishing-filter til (9)**. Så vil Microsoft automatisk tjekke alle de websteder, du prøver at gå ind på. De bliver sammenlignet med en liste over kendte svindel-websteder, og du bliver advaret, hvis dine sider findes på listen.





5: Hængelåsen koder kommunikationen

Hvis du ser et ikon af form som en **hængelås (10)** ved siden af en webside i adressefeltet, betyder det, at din kommunikation med webstedet er kodet. Derfor kan andre ikke læse, hvad der sendes mellem dig og webstedet – hvilket kan være rigtig rart, fx i forbindelse med din netbank eller din e-mail-konto. Hængelåsen er et bevis på, at du faktisk kommunikerer med det websted, hvis navn står i adressefeltet, og du kan klikke på den for at læse flere informationer om webstedet.

Hacker: Person, som uden tilladelse bryder ind på en anden computer. Hackere kan lave indbruddet for at skaffe sig adgang til informationer, stjæle programmer eller simpelt hen som en intellektuel udfordring.

Brug flere browsere

De fleste angreb er rettet mod Internet Explorer, og hvis din browser bliver angrebet, kan det medføre, at angriberne får adgang til information fra andre websteder, du har åbnet med samme browser. Derfor kan det være en idé at bruge to browsere: Benyt fx Internet Explorer til de udvalgte websteder, som du har fuld tillid til: din netbank, SKATs TastSelv-tjeneste, din læge og lignende. Alle andre websteder kan du så besøge med browserne Firefox, Opera eller Safari.
Hent Firefox: **www.getfirefox.com**
Hent Opera: **www.opera.com**
Hent Safari: **www.apple.com/safari/**

Kendte websteder kan også være farlige

Selv om du har tillid til et websted, kan det godt være farligt. Det skyldes, at hackere i sjældne tilfælde kan lægge skadelige programmer ind på det, fx i nogle reklamer. Hvis du besøger webstedet med en browser, der ikke er opdateret, kan din pc blive inficeret med virus og andet bras. Kendte websteder som Børsen, Ekstra Bladet og TV 2 har således været med til at sprede skadelige programmer, fordi hackere havde infiltreret deres websider.

Vidste du det? Den nyeste browser fra Microsoft hedder Internet Explorer 7 – og det er den, vi fortæller om på disse sider. Internet Explorer 7 er mere sikker og hurtigere end sine forgængere, og hvis du ikke allerede har den på din pc, kan du hente den gratis her: **www.microsoft.dk/ie**



Din personlige underskrift på nettet

Den digitale signatur er – som navnet antyder – en slags elektronisk udgave af din underskrift. På samme måde, som du skriver under på et brev, en kontrakt eller en anden form for aftale med din almindelige signatur, så kan du bruge den digitale signatur til at identificere dig på nettet. Men hvordan virker det egentlig? Her får du svar på alt om den digitale signatur. Af Thomas O. Nielsen

Hvad er en digital signatur?

Er dette første gang du stifter bekendskab med en digital signatur, er det sikkert nærliggende at forestille sig en indscannet underskrift, der fx kan vedhæftes dine e-mails. Men den digitale signatur er i virkeligheden langt mere avanceret og består af to såkaldte nøgler: en privat og en offentlig nøgle.

Den private nøgle er en fil, som du opbevarer på din pc, og som du kan bruge til at identificere dig på nettet. For at kunne anvende den private nøgle skal du angive en adgangskode, som sikrer, at andre ikke kan anvende din personlige nøgle, selv om de får adgang til din computer. Med den private nøgle installeret på pc'en kan du logge ind på en række offentlige og private hjemmesider med én og samme adgangskode. Du kan også bruge din private nøgle til at underskrive dine e-mails, så modtageren har vished for, at den virkelig stammer fra dig.

Ved udstedelsen af den private nøgle laves der også en offentlig nøgle, som opbevares af den udstedende myndighed. Den offentlige nøgle kan

På **www.digitalsignatur.dk** kan du nemt bestille din egen digitale signatur. Bare klik på **Bestil digital signatur** (1), og følg anvisningerne.

hentes af alle og enhver og kan blandt andet anvendes af modtageren til at få sikkerhed for, at din signatur i en e-mail er gyldig, og at der ikke er blevet ændret på indholdet, siden du signerede e-mailen. På samme måde anvendes den offentlige nøgle til at godkende dig, når du logger ind på en hjemmeside med din private nøgle.

Hvem står for den digitale signatur?

Den digitale signatur administreres af IT- og Telestyrelsen, som er en styrelse under Ministeriet for Videnskab, Teknologi og Udvikling. Håndteringen og udstedelsen af digitale signaturer i Danmark har siden 2003 været udliciteret til TDC.

Hvad kan jeg bruge den til?

Med din digitale signatur kan du kommunikere med det offentlige 24 timer i døgnet og få et bedre overblik over informationer – og så kan du slippe for at skrive et brev i hånden eller på computeren, printe det ud, finde en konvolut, købe et frimærke, gå til postkassen med det og derefter vente på svar. Du kan blandt meget andet bruge din digitale signatur på: eBoks, FerieKonto, Sygeforsikringen danmark, SKAT, Statens Uddannelsesstøtte, Sundhed.dk og hos alle kommuner.
Se den komplette liste på **www.digitalsignatur.dk**

Kan jeg bruge min digitale signatur på en anden pc end min egen?

Du kan installere din digitale signatur på en hvilken som helst computer, men vi fraråder på det kraftigste at gøre det på computere, som andre end du og din nærmeste familie har adgang til.

Er den digitale signatur lige så gyldig som en underskrift?

Ja! Den digitale signatur er i princippet lige så juridisk bindende som en traditionel, håndskreven underskrift.

Hvor sikker er den?

Et kritikpunkt ved den digitale signatur har været, at sikkerheden i høj grad beror på, hvor godt brugeren passer på sin private nøgle – og dermed også hvor godt hans eller hendes computer er sikret. Der er dog ingen tvivl om, at den digitale signatur er langt, langt mere sikker end almindelig brug af brugernavn og adgangskode på hjemmesider, og Datatilsynet har godkendt signaturen til sikker kommunikation mellem borgere, virksomheder og myndigheder.

Hvad gør jeg, hvis andre får adgang til min signatur?

Får du stjålet den computer, hvor din private nøgle er installeret, eller skulle andre på anden vis få adgang til din digitale signatur, er det vigtigt at tage sine forholdsregler. Selv om den private nøgle er beskyttet af en adgangskode, så bør du handle, nøjagtig som hvis dit dankort blev stjålet: Få signaturen spærret. Du ringer til TDC's døgnåbne spærrelinje på 80 80 16 16 og opgiver din spærringskode, som stod i det brev, du fik tilsendt, da du bestilte din digitale signatur. Er brevet blevet væk, skal du opgive dit CPR-nummer.

Hvad gør jeg, hvis jeg glemmer adgangskoden?

Din underskriftskode er personlig, og det er kun dig, der kender den. Derfor bliver du nødt til at bestille en ny digital signatur på adressen **www.digitalsignatur.dk**

Kan hele familien bruge én digital signatur?

Nej. Den digitale signatur er din personlige underskrift, og det betyder, at den er til din personlige brug. Hvis en anden i familien ønsker at bruge digital signatur, skal han eller hun have sin egen. Der kan sagtens installeres flere digitale signaturer på samme pc.

Hvordan får jeg en digital signatur?

Du kan bestille din egen digitale signatur på www.digitalsignatur.dk – og det er både nemt og ganske gratis for alle danskere med folkeregisteradresse i Danmark. Signaturen bestilles ved at indtaste CPR-nummer, postnummer og din e-mail, hvorefter du modtager en e-mail med et link til installation af din digitale signatur. Dette link kan dog først anvendes, når du efter et par arbejdsdage modtager et papirbrev med din midlertidige pinkode. Brevet sendes til den adresse, der i Folkeregisteret er registreret for dit CPR-nummer, og på den måde sikres det, at ingen andre kan bestille en signatur i dit navn. Når pinkoden er modtaget, kan den digitale signatur installeres gennem få trin, som du kan læse mere om i den e-mail, du modtager ved bestilling.

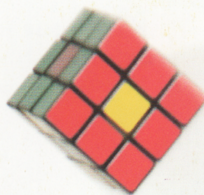
Ny digital signatur på vej

Den eksisterende digitale signatur har efterhånden fem år på bagen, og med de erfaringer, man har gjort sig, er en ny version nu på vej. Den nye digitale signatur adskiller sig væsentligt fra den gamle, idet den private nøgle ikke længere opbevares på brugerens egen computer, men på en central server. Den nye digitale signatur er ligesom den gamle tilknyttet en adgangskode, men herudover er adgangen til den private nøgle yderligere beskyttet af en engangskode. Ved oprettelse af den nye digitale signatur modtager brugeren et plastickort med påtrykte engangskoder, og når de er brugt, fremsendes et nyt automatisk. Det vil gøre det muligt at anvende den digitale signatur fra en hvilken som helst computer uden at skulle installere sin private nøgle først. Den nye digitale signatur forventes taget i brug over de kommende to år, men foreløbig kan du roligt fortsætte med at bruge din nuværende signatur – eller bestille en, hvis du ikke har gjort det endnu.

Vidste du det?

Du kan få hjælp til at installere din digitale signatur, sikkerhedskopier, adgangskoder osv. ved at ringe til TDC's gratis support på 80 80 15 81. TDC svarer også på generelle spørgsmål om brugen af digital signatur.

Er du sikker på nettet?



Nu har du chancen for at teste din viden om sikker adfærd ved pc'en – og finde ud af, hvor godt rustet du er til at bevæge dig sikkert rundt på internettet.

10 skarpe spørgsmål:

1. Hvad kendetegner en god adgangskode?

a) Koden er lang og består af tal, specialtegn samt store og små bogstaver.
b) Koden er simpel og let at huske, fx navnet på den by, du bor i.
c) Koden indeholder bogstaver fra både det kyrilliske og det latinske alfabet.

2. Hvad er en trojansk hest?

a) Et ondsindet computerprogram, der åbner en "bagdør" til din pc.
b) Navnet på et førende antivirusprogram.
c) Snu spyware, der kan springe over en firewall.

3. Du modtager en mail fra din bank, hvor du bliver bedt om at indtaste dine kontooplysninger. Hvad gør du?

a) Indtaster oplysningerne og returnerer mailen til din bank.
b) Sletter mailen (din bank vil ikke afkræve dig fortrolige oplysninger på mail).
c) Skriver mailen ud og sender oplysningerne med et brev til banken.

4. Du tilmelder dig et nyhedsbrev på en hjemmeside. Hvor meget bør du oplyse?

a) Din e-mail-adresse.
b) Din e-mail-adresse og postadresse.
c) Din e-mail-adresse, postadresse og dine bankoplysninger.

5. Hvad er phishing?

a) Et forsøg på at lokke fortrolige oplysninger fra dig.
b) Sletning af skadelige filer på pc'en.
c) En FBI-metode til at afsløre hackere.

6. Hvad gør et spamfilter?

a) Sender mails til alle på en adresseliste i fx Outlook Express.
b) Spærrer for pornografisk materiale på nettet.
c) Spærrer for uønskede reklame-e-mails.

7. Hvordan opdaterer du dit antivirusprogram?

a) Opdateringen foregår via internettet. Det sker automatisk – typisk en gang om dagen.
b) Hvis programmet er godt nok, behøver du ikke opdatere det.
c) Opdatering foregår en gang cirka hvert halve år i en såkaldt Service Pack.

8. Hvad betyder det, at en hjemmesides webadresse indledes med "https" i stedet for blot "http"?

a) At hjemmesiden er godkendt af Videnskabsministeriet.
b) At hjemmesiden bruger en sikker protokol til at overføre data.
c) At siden ejes af en skandinavisk virksomhed.

9. Hvad beskytter en firewall dig mod?

a) Hackere og orme.
b) Museskader.
c) Tyveri af pc-udstyr i hjemmet.

10. Hvordan hjælper en digital signatur din færden på nettet?

a) En digital signatur sætter flueben ud for sikre søgeresultater, fx i Google.
b) Programmet Digital Signatur indtaster automatisk dine data i online-formularer, så du sparer tid.
c) Den digitale signatur er en adgangskode, der gør det lettere at kommunikere med både private virksomheder og offentlige institutioner.

De rigtige svar: 1: a/2: a/3: b/4: a/5: a/6: c/7: a/8: b/9: a/10: c

Hvordan klarede du dig?

9-10 rigtige: Ekspert: Rigtig god fornøjelse på nettet – du har tjek på sikkerheden.
6-8 rigtige: Rutineret: Du kan roligt bevæge dig ud på nettet, så længe du tager din kritiske sans med dig.
3-5 rigtige: På vej: Hold foden på bremsen, hvis du går på nettet, og besøg kun sider, du har tillid til. Hackere ligger på lur for at kaste sig over novicer som dig.
0-2 rigtige: Begynder: Det er nok en god idé at gå på nettet sammen med en ven, indtil du har sat dig godt ind i de faldgruber, der venter dig.

Vil du vide mere?

Der er meget mere inspiration og viden om sikkerhed på nettet at hente i dette magasin og på hjemmesiderne **www.netsikkernu.dk**, **www.opdaterdinpc.dk** og **www.komputer.dk/netsikker** – rigtig god fornøjelse!